

AG2 ✓

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-190810

(P2002-190810A)

(43) 公開日 平成14年7月5日(2002.7.5)

(51) Int.Cl. ⁷	識別記号	F I	ターミナル* (参考)
H 0 4 L 12/28		C 0 6 F 13/00	3 5 3 B 5 B 0 8 9
G 0 6 F 13/00	3 5 3	H 0 4 L 11/00	3 1 0 D 5 K 0 3 0
H 0 4 L 12/66		11/20	B 5 K 0 3 3

審査請求 未請求 請求項の数 8 O L (全 18 頁)

(21) 出願番号 特願2000-393280(P2000-393280)

(22) 出願日 平成12年12月21日(2000. 12. 21)

(71) 出願人 000003108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 柴田 淳司

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

(74) 代理人 100076096

弁理士 作田 康夫

Fターム(参考) 5B089 GA19 GB02 HB06 JB14 KB04

5K030 HD08 HD09 MD07

5K033 CB09 EC04

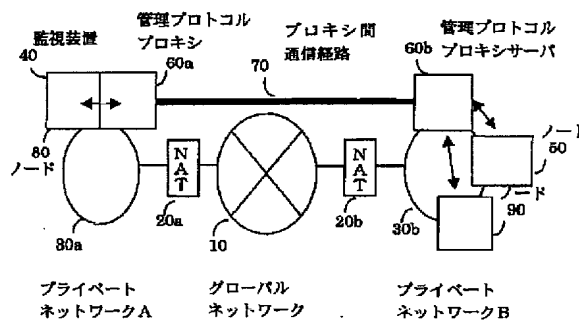
(54) 【発明の名称】 ネットワーク管理システム

(57) 【要約】

【課題】グローバルアドレスを持たないノード間でデータ通信を行うこと。

【解決手段】アドレス体系が異なる第1のネットワークと第2のネットワークとがアドレス変換装置を介して接続されたネットワークシステムを管理するネットワーク管理システムであって、第1、第2のネットワークは、それぞれノード及び管理プロトコルプロキシとを有し、それぞれの管理プロトコルプロキシは、ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニットをデータとする管理プロトコルプロキシデータとする管理プロトコルプロキシデータ生成部と、他の管理プロトコルプロキシから送られてきた管理プロトコルプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換するアドレス変換部とを有する。

図1



【特許請求の範囲】

【請求項1】アドレス体系が異なる第1のネットワークと第2のネットワークとがアドレス変換装置を介して接続されたネットワークシステムを管理するネットワーク管理システムであって、

前記第1、第2のネットワークは、それぞれノード及び管理プロトコルプロキシとを有し、

それぞれの前記管理プロトコルプロキシは、ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニットをデータとする管理プロトコルプロキシデータとする管理プロトコルプロキシデータ生成部と、他の管理プロトコルプロキシから送られてきた管理プロトコルプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換するアドレス変換部とを有するネットワーク管理システム。

【請求項2】前記管理プロトコルプロキシは、ノードから送られてきた管理プロトコルのパケットに含まれる送信先アドレスと管理プロトコルプロキシのアドレスとを対応付けしたアドレス定義情報を有し、前記管理プロトコルプロキシデータ生成部は、ノードから送られてきた送信先アドレスと前記アドレス定義情報から送信先の管理プロトコルプロキシのアドレスを決定する請求項1記載のネットワーク管理システム。

【請求項3】前記第1又は第2のネットワークの少なくとも一方のネットワークの前記管理プロトコルプロキシが有するアドレス定義情報は、前記アドレス変換装置で定義されないアドレスと管理プロトコルプロキシのアドレスとが対応付けて定義されている請求項1記載のネットワーク管理システム。

【請求項4】前記管理プロトコルのプロキシは、アドレス変換情報を定義したアドレス変換ルールを有し、前記アドレス変換部は、前記アドレス変換ルールと変換の対象となるMIBオブジェクトのASN.1定義文により、管理プロトコルのプロトコルデータユニットに含まれるアドレス情報を変換する請求項2記載のネットワーク管理システム。

【請求項5】アドレス体系が異なる複数のネットワークがアドレス変換装置で接続されたネットワークシステムを管理するネットワーク管理システムであって、それぞれのネットワークに接続された複数のノード及び複数の管理プロトコルプロキシとを有し、それぞれの前記管理プロトコルプロキシは、ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニット内のデータを管理プロトコルのプロキシデータとする管理プロトコルプロキシデータ生成部と、他の管理プロトコルプロキシから送られてきた管理プロトコルのプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換するアドレス変換部とを有するネット

ワーク管理システム。

【請求項6】ノードから送られてきたパケットを処理して送信する管理プロトコルの処理方法であって、ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニット内のデータを管理プロトコルのプロキシデータとし、他の管理プロトコルプロキシから送られてきた管理プロトコルのプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換する管理プロトコルの処理方法。

【請求項7】ノードから送られてきた管理プロトコルのパケットを処理して送信する管理プロトコルの処理が記憶されたコンピュータ読み取り可能な記憶媒体であって、

ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニット内のデータを管理プロトコルのプロキシデータとし、他の管理プロトコルのプロキシから送られてきた管理プロトコルのプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換する処理が記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項8】ノードから送られてきた管理プロトコルのパケットを処理して送信する管理プロトコルの処理を行うプログラムであって、

ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニット内のデータを管理プロトコルのプロキシデータとし、他の管理プロトコルのプロキシから送られてきた管理プロトコルのプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換するプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク管理システムに係り、特に、互いにアドレス体系が異なる複数のネットワークが接続されたネットワークシステムを管理するネットワーク管理システムに関する。

【0002】

【従来の技術】現在、インターネットなどで最も広く利用されているネットワークアドレスであるIPアドレスは、IPv4 (Internet Protocol ver.4) と呼ばれるプロトコルにより規定されるもので、32ビットのアドレス空間を持つアドレスである。ネットワークアドレスは、ネットワークに接続される機器に一意に割り当てられていなければならない、インターネットに接続する機器のネットワークアドレスについてはNICと呼ばれる機関などにより一意になるように割り当てが行われてきた。IPv4では、32ビットのアドレス空間を持つので理論的には最大で2の32乗個すなわち40億ものアドレスを割り当てることができる。しかしながら、インターネットに接続

する機器が増加すると、インターネットに接続する全ての機器にIPv4のIPアドレスを割り当てることが困難になる。

【0003】この問題を解決するための技術として広く使われているのが、IETFの定めるRFC1631(The IP Network Address Translator)に記載されているアドレス変換機能と、RFC1918(Address Allocation for Private Internets)に記載されているプライベートネットワークとを組み合わせた方法である。この方法は、例えば企業内ネットワークなどのローカルなネットワーク内に存在する全ての機器が必ずしもインターネットなどの外部のネットワークに接続するとは限らないということを前提としている。すなわち、まず企業内ネットワークなどのローカルなネットワークは、RFC1918に記載されたプライベートアドレスの範囲のアドレスを使用してIPアドレスを割り当ててネットワークを構築する。このとき、このプライベートアドレスでは、インターネットなどの外部ネットワークには接続しないようにする。インターネットなどの外部ネットワークに接続する機器については、ローカルのネットワークとインターネットなどの外部ネットワークとの間に、RFC1613に記載されたアドレス変換装置を配置し、アドレス変換により送受信パケットのアドレスをプライベートアドレスから、インターネットにアクセスするためのグローバルアドレスへと変換することによって、接続を可能とする。ここでグローバルアドレスとはNICなどにより割り当てられたアドレスである。このとき、グローバルアドレスを動的に割り当てて、複数のローカルノードが時間割で1つのグローバルアドレスを共有できるようにするなど、有限であるグローバルアドレスを有効に活用するような工夫も行われている。

【0004】ところで、RFC1631において記載されるアドレス変換においては、IPパケットのヘッダに含まれる送信元と送信先のIPアドレスの書き換えと、それに伴って生じるIPヘッダのチェックサムの変更を再計算して置き換える。これによってTCP/IPによる通信が可能となり、その上位層のプロトコルによる通信も可能になる。

【0005】しかしながら、例えばSNMPなどのネットワーク管理プロトコルにおいては、管理プロトコルによってやりとりされるプロトコルデータユニット(PDU)中にもIPアドレスが含まれているが、この部分はRFC1631に記載されるアドレス変換装置においては、アドレス変換されない。

【0006】一方、特開平11-187058号公報には、RFC1631に記載されるアドレス変換の機能に加えて、管理プロトコルのプロトコルデータユニットについてもアドレス変換をするようなアドレス変換装置が記載されている。

【0007】

【発明が解決しようとする課題】しかしながら、アドレ

ス変換装置によってプライベートアドレスとグローバルアドレスによる運用を行うと、管理装置側のネットワークで使用できるグローバルアドレスを用いた管理プロトコルの通信によって行われることになる。このため、被監視側にあつてグローバルアドレスを割り当てられているノードに対してだけしか、管理プロトコルによる通信を行うことができない。しかしながら、ネットワーク管理においては、そのようなグローバルアドレスを持たないノードについても管理を行うことができれば、より有効な管理を行うことが可能となる。特開平11-187058の方法では、この点については開示されていない。

【0008】本発明の目的は、異なるアドレス体系のネットワークがアドレス変換装置により接続されたネットワークシステムにおいて、グローバルアドレスを持たないノード間でも管理プロトコルによるデータ通信が行えるネットワーク管理システムを提供することにある。

【0009】

【課題を解決するための手段】上記目的を達成する一手段として、アドレス体系が異なる第1のネットワークと第2のネットワークとがアドレス変換装置を介して接続されたネットワークシステムを管理するネットワーク管理システムであつて、第1、第2のネットワークは、それぞれノード及び管理プロトコルプロキシとを有し、それぞれの管理プロトコルプロキシは、ノードから送られてきた管理プロトコルのパケットに含まれる送信元アドレス、送信先アドレス、プロトコルデータユニットをデータとする管理プロトコルプロキシデータとする管理プロトコルプロキシデータ生成部と、他の管理プロトコルプロキシから送られてきた管理プロトコルプロキシデータに含まれるプロトコルデータユニット内のアドレス情報を変換するアドレス変換部とを有する。

【0010】これにより、管理プロトコルのプロキシ間でデータ通信を行うことができ、グローバルアドレスを持たないノード間でデータ通信を行うことができる。

【0011】

【発明の実施の形態】以下、図面に従つて管理プロトコルにSNMPを適用した場合の実施例を説明する。図1は、本実施例で説明するネットワーク管理システムの概念を示したものである。

【0012】本システムは、グローバルネットワーク10、プライベートネットワークA30a、プライベートネットワークB30bとを有しており、プライベートネットワークA30aとグローバルネットワーク10とをアドレス変換を行うNAT20a、プライベートネットワークB30bとグローバルネットワーク10とをアドレス変換を行うNAT20bによって接続している。

【0013】プライベートネットワークA30aには、監視を行うためのノード80が接続されている。このノード80は、被監視装置を監視するための処理を行う監

視装置40と、管理プロトコルのプロキシデータの生成、プロキシデータに含まれるプロトコルデータユニット内のアドレス変換などを行う管理プロトコルプロキシ60aを有している。

【0014】また、プライベートネットワークB30bには、被監視装置であるノード50、90、管理プロトコルのプロキシデータの生成、プロキシデータに含まれるプロトコルデータユニット内のアドレス変換などを行う管理プロトコルプロキシサーバ60bが接続されている。

【0015】このような構成において、本ネットワーク管理システムは、監視を行うためのノード80が、被監視装置であるノード50、90を管理するものである。

【0016】プライベートネットワークA30aのノード80の監視装置40によって被監視装置であるノード50とデータ通信を行う場合、ノード80の管理プロトコルプロキシ60aとプライベートネットワークB30bの管理プロトコルプロキシサーバ60bとの間でデータ通信を行うようにする。これは、プロキシ間通信経路70と呼ぶ仮想的な通信経路を形成したことに等価になる。

【0017】このようにすれば、プライベートネットワークA30aで使用されるアドレスと、プライベートネットワークB30bで使用されるアドレスとが異なる場合、つまり異なったアドレス体系のネットワーク間でデータ通信を行うことができる。また、プライベートネットワークA30aと、プライベートネットワークB30bとの間にプライベートネットワークのアドレスや、グローバルネットワークのアドレスを通過させないファイアウォールなどが形成されている場合でもデータ通信を可能とすることができる。

【0018】より具体的に図1に示したネットワークシステム全体の動作について説明する。図2は、ノードの管理プロトコルSNMPのSNMPメッセージパケットを示したものである。図3は、管理プロトコルプロキシサーバの管理プロトコルプロキシデータの packets を示したものである。すなわち、ノード80の監視装置40、被監視装置であるノード50、ノード90から送信される管理プロトコルSNMPの packets から管理プロトコルプロキシ60a、管理プロトコルプロキシサーバ60bは、ネットワーク層であるIP層のヘッダ中の送信先、送信元として保持されていた送信元、送信先情報を、アプリケーション層のデータにあたる管理プロトコルプロキシデータの中に格納する。更に、管理プロトコルプロキシデータの packets のトランスポート層としてはコネクション型の例えばTCPを用いる。また、管理プロトコルプロキシデータ自体の送信先、送信元は、管理プロトコルプロキシ又は管理プロトコルプロキシサーバとなる。

【0019】ここで、監視装置40から被監視装置であ

るノード50又はノード90へ、またその反対の被監視装置であるノード50又はノード90から監視装置40へと、管理プロトコルプロキシ60a、管理プロトコルプロキシサーバ60bを介して通信が行われるときのデータの流れについて説明する。監視装置であるノード40が送信した管理プロトコルのデータが管理プロトコルプロキシ60aに届けられると、管理プロトコルプロキシ60aは、管理プロトコルのデータそのものと、管理プロトコルのデータの本来の送信先、送信元を組み合わせ管理プロトコルプロキシデータを生成し、管理プロトコルプロキシデータを管理プロトコルプロキシサーバ60bへ送信する。管理プロトコルプロキシサーバ60bは受信した管理プロトコルプロキシデータから、管理プロトコルのデータと、本来の送信先とを取り出して、管理プロトコルの packets を再構築し、本来の送信先である被監視装置であるノード50へ送信する。このとき、管理プロトコルの packets の送信元を管理プロトコルプロキシサーバ60bとしておくことで、ノード50からの応答が管理プロトコルプロキシサーバ60bに送信される。ノード50からの管理プロトコルの応答 packets を受信した管理プロトコルプロキシサーバ60bは、その応答 packets を管理プロトコルプロキシデータに変換し、管理プロトコルプロキシ60aに送り返す。管理プロトコルプロキシ60aは、管理プロトコルプロキシデータから管理プロトコルの応答 packets を再構築し、監視装置40に返す。

【0020】以上のようにして、ノード間で管理プロトコルを使用して直接通信できない環境において、管理プロトコルプロキシ、管理プロトコルプロキシサーバを介することで管理プロトコルによる通信を行うことができるようになる。

【0021】更に、管理プロトコルプロキシ、管理プロトコルプロキシサーバは、管理プロトコルのPDU部分のアドレスを変換するアドレス変換機能を有している。これにより、ノードの管理プロトコルのプロトコルデータユニット（以下、「PDU」と称す。）中に含まれるノードのアドレスを、ネットワーク管理用の仮想的なアドレスに変換することによって、ノードがあたかも仮想的なアドレスを持つかのように管理することができる。このときのネットワーク管理においてのみ使用される仮想的なアドレスを便宜上、本実施例では「管理用アドレス」と呼ぶ。

【0022】尚、図1で示した構成においては、管理プロトコルプロキシ60aをプログラムで実現する場合について説明したが、管理プロトコルプロキシサーバ60bの機能も同様にプログラムによって実現することができる。この場合は、コンピュータで読み取り可能な磁気ディスク、光ディスク、光磁気ディスクにプログラムを記録し、管理プロトコルプロキシサーバの機能を担当するノードが、プログラムを読み出して実行する。

【0023】次に、図1に示したNATについて説明する。図1に示したNATはRFC1631に準拠したものである。図4はNATの機能を説明するための図である。この図に示すように、グローバルネットワーク10とプライベートネットワーク30がNAT20を介して接続されているネットワークにおいて、ノード40はグローバルアドレス200としてG0が割当てられ、被監視装置はプライベートアドレス210としてL1が、グローバルアドレスとしてG1が割り当てられている場合について説明する。この場合、そのグローバルアドレスと、プライベートアドレスの対応づけた変換表230をNAT20に設ける。これにより、ノード40側からノード50側にアドレスG1に対してパケットを送信する。NAT20はアドレスG1へ向けたパケットを変換表230に従って送信先アドレスをG1からL1へと変換して、プライベートネットワーク側へ送信する。すなわち、図5のようにノード40側からNAT20へ到着したパケットとしては、ネットワーク層に相当するIP層部分のヘッダ情報として送信先はG1という情報が入っていたパケットだったものが、NAT20からプライベートネットワーク側のノードに向けて中継されるときには、図6のようにIP層部分のヘッダ情報として送信先はL1という情報が入ったパケットとなって送信される。また、逆にプライベートネットワーク側のノード50からグローバルネットワーク側のノード40へ向けてパケットを送信する場合は、ノード50からNAT20へ到着したパケットとしてはIP層部分のヘッダ情報として送信元はL1という情報が入っていたパケットだったものが、NAT20からグローバルネットワーク側のノード40に向けて中継されるときには、IP層部分のヘッダ情報として送信元はG1という情報が入ったパケットとして送信される。

【0024】このようなNAT20の働きにより、ノード50自身のネットワークの設定としてはプライベートアドレスL1を持つものとして設定するだけでよく、ノード50とプライベートネットワーク内の他の装置とが通信する場合にはプライベートアドレスL1を使用して通信でき、さらにグローバルネットワーク側の装置との間で通信を行う場合には、NAT20によって割り当てたグローバルアドレスG1を使用して通信できる。

【0025】尚、ここではNATはIP層のアドレス変換を行う機能を有するもの（管理プロトコルのPDU部分のアドレス変換は行えない。）として説明した。このようなNATを利用したネットワークにおいて、既に説明したように管理プロトコルプロキシサーバにおいて、管理プロトコルのPDU部分のアドレスを変換するものである。

【0026】以下、より具体的なネットワークシステムについて説明する。図7は、ネットワーク管理システムにおける適用例の1つであり、被監視側装置に割り当て

られた正式なグローバルアドレスをネットワーク管理用のアドレスとして使用して管理する場合の構成である。

【0027】被監視装置a 50aは、プライベートアドレス210としてL1を持っている。このL1というアドレスは、プライベートアドレスであるので、プライベートネットワークB 30bの中だけで使用できるアドレスである。

【0028】さらに、NAT20bにおけるアドレス変換230として、グローバルアドレスG1とプライベートアドレスL1が対応付けられており、被監視装置a 50aにはグローバルアドレスとしてアドレスG1が静的に割り当てられている。グローバルネットワーク10やプライベートネットワークA 30aから被監視装置a 50aと直接通信する場合には、グローバルアドレスG1を用いて通信する。

【0029】ここで、管理プロトコルプロキシ60bにおけるアドレス変換220として、管理用アドレスG1とプライベートアドレスL1を対応付けることで、監視側から被監視側に送られる管理プロトコルデータについては、G1をL1に、被監視側から監視側へ送られる管理プロトコルデータについては、L1をG1に、それぞれ変換する。

【0030】これにより、監視装置側から管理プロトコルを使用して管理プロトコルのデータを参照すると、あたかも被監視装置a 50aがアドレスG1を持っているかのように見える。

【0031】このため監視装置40における管理情報240としては、被監視装置aはアドレスG1を持つ装置であるに対応付けられ、アドレスG1を使ってネットワーク管理を行うことができる。

【0032】次に図8は、NAT20bによって被監視装置に割り当てられるグローバルアドレスが動的に割り当てられる場合である。一般に、NATによって接続されたプライベートネットワークにおいて外部接続のために使用できるグローバルアドレスの数は、プライベートネットワーク内の装置の数より少ない。少ないグローバルアドレスを有効に活用するための方法として、装置に対するグローバルアドレスの割り当てを、その装置が外部に接続している間だけ割り当てるようにし、その装置が外部への接続を終了したならば、その装置が使用していたグローバルアドレスを他の装置によって再利用されるようにする方法を使用する。このようにグローバルアドレスを動的に割り当てる場合、一般的にはある1つの装置に割り当てられるグローバルアドレスは、その時により異なる。

【0033】このような場合、NAT20bにおけるアドレス変換230として、グローバルアドレスGxとプライベートアドレスL1が対応付けられており、Gxはその時々により一定の選択肢のアドレスの中から選択して選ばれるアドレスであり、少なくともその時点におい

ては被監視装置 a 50 a にはグローバルアドレスとしてアドレス Gx が動的に割り当てられていることになる。どのようなアドレスが割り当てられるかは NAT 20 b により決定される。

【0034】ここで仮に、Gx を管理用アドレスとしてそのまま使うとすると、監視装置 40 における管理情報 240 として被監視装置 a 50 a に対応づけられたアドレスがその時々で変わってしまい、管理の継続性が維持できず正しいネットワーク管理が行えないため、問題である。

【0035】そこで、図 8 のように管理プロトコルプロキシ 60 b におけるアドレス変換 220 としては、Gx とは全く別の V1 という仮想的なアドレスを静的に割り当てるようにする。これにより、監視装置における管理情報 240 としては、被監視装置 a はアドレス V1 を持つものと対応づけられるため、正しくネットワーク管理を行うことができる。

【0036】図 9 は、被監視側のプライベートネットワークが複数あり、それらプライベートネットワーク内の被監視装置のプライベートアドレスが競合している場合の例である。

【0037】被監視装置 b 50 b は、プライベートネットワーク B 30 b に存在し、プライベートアドレス L1 を持つ。被監視装置 c 50 c は、プライベートネットワーク C 30 c に存在し、プライベートアドレス L1 を持つ。互いのアドレスが競合しているが、プライベートアドレスは、通信上はそのプライベートネットワーク内でしか使われないため、ネットワークが混乱することはない。

【0038】しかしながら仮に、被監視装置 b 50 b および被監視装置 c 50 c から直接管理プロトコルを使って管理プロトコルのデータを取得すると、そのどちらもがアドレス L1 を持つ装置としての情報を応答するため、監視装置が混乱してしまい正しくネットワーク管理ができないという問題が発生する。

【0039】そこで図 9 のように、被監視装置 b 50 b については、管理プロトコルプロキシ 60 b におけるアドレス変換 220 b において管理用アドレス V1 とプライベートアドレス L1 とを対応づけるようにし、被監視装置 c 50 c については、管理プロトコルプロキシ 60 c におけるアドレス変換 220 c において管理用アドレス V2 とプライベートアドレス L1 とを対応づけるようにする。すなわち被監視装置 b 50 b に管理用アドレス V1 と、被監視装置 c 50 c に管理用アドレス V2 をそれぞれ静的に割り当てるようにする。

【0040】これによって監視装置における管理情報 240 としては、被監視装置 b は、アドレス V1 を持つ装置として、被監視装置 c は、アドレス V2 を持つ装置として、それぞれ対応づけられ、正しくネットワーク管理を行うことができる。

【0041】図 10 は、プライベートネットワークにおいて、グローバルアドレスが割り当てられていない、すなわち外部とは接続しない装置に対しても、管理用アドレスを割り当ててネットワーク管理する場合の例である。

【0042】被監視装置 a 50 a は、プライベートアドレス 210 a として L1 を持つ。さらに、NAT 20 b におけるアドレス変換 230 として、グローバルアドレス G1 とプライベートアドレス L1 が対応付けられており、被監視装置 a 50 a にはグローバルアドレスとしてアドレス G1 が静的に割り当てられている。グローバルネットワーク 10 やプライベートネットワーク A 30 a から被監視装置 a 50 a と直接通信する場合には、グローバルアドレス G1 を用いて通信する。

【0043】被監視装置 b 50 b は、プライベートアドレス 210 b として L2 を持つ。しかしながら、NAT 20 b におけるアドレス変換 230 としては、プライベートアドレス L2 に対応するグローバルアドレスは定義されておらず、このため、グローバルネットワーク 10 やプライベートネットワーク A 30 a から被監視装置 b 50 b へと直接通信することはできない。ただし、この場合でも管理プロトコルプロキシを通じて、監視装置 40 は、被監視装置 50 b ととも管理プロトコルによる情報のやり取りをすることができる。

【0044】このとき、管理プロトコルプロキシ 60 b におけるアドレス変換 220 において、管理用アドレス V1 とプライベートアドレス L1 とを、管理用アドレス V2 とプライベートアドレス L2 とを、それぞれ対応づけるようにする。すなわち被監視装置 a 50 a に管理用アドレス V1 を、被監視装置 b 50 b に管理用アドレス V2 をそれぞれ静的に割り当てるようにする。これにより、監視装置における管理情報 240 としては、被監視装置 a 50 a はアドレス V1 を持つ装置として、被監視装置 b 50 b はアドレス V2 を持つ装置として、それぞれ対応付けられてネットワーク管理が行われる。

【0045】図 11 は、プライベートネットワークにおいて、グローバルアドレスが割り当てられていない、すなわち外部とは接続しない装置に対しても、管理用アドレスを割り当ててネットワーク管理する場合において、グローバルアドレスを割り当てられている装置については、管理用アドレスにグローバルアドレスを使い、グローバルアドレスが割り当てられていない装置については仮想的なアドレスを使う例である。

【0046】被監視装置 a 50 a は、プライベートアドレス 210 a として L1 を持つ。さらに、NAT 20 b におけるアドレス変換 230 として、グローバルアドレス G1 とプライベートアドレス L1 が対応付けられており、被監視装置 a 50 a にはグローバルアドレスとしてアドレス G1 が静的に割り当てられている。グローバルネットワーク 10 やプライベートネットワーク A 30 a

から被監視装置a50aと直接通信する場合には、グローバルアドレスG1を用いて通信する。

【0047】被監視装置b50bは、プライベートアドレス210bとしてL2を持つ。しかしながら、NAT20bにおけるアドレス変換230としては、プライベートアドレスL2に対応するグローバルアドレスは定義されておらず、このため、グローバルネットワーク10やプライベートネットワークA30aから被監視装置b50bへと直接通信することはできない。ただし、この場合でも管理プロトコルプロキシを通じて、監視装置40は、被監視装置50bとも管理プロトコルによる情報のやり取りをすることができる。

【0048】このとき、管理プロトコルプロキシ60bにおけるアドレス変換220において、管理用アドレスG1とプライベートアドレスL1とを、管理用アドレスV2とプライベートアドレスL2とを、それぞれ対応づけるようにする。すなわち被監視装置a50aに管理用アドレスG1を、被監視装置b50bに管理用アドレスV2をそれぞれ静的に割り当てるようにする。これにより、監視装置における管理情報240としては、被監視装置a50aはアドレスG1を持つ装置として、被監視装置b50bはアドレスV2を持つ装置として、それぞれ対応付けられてネットワーク管理が行われる。

【0049】続いて図12および図13を用いて、管理プロトコルプロキシの構成を説明する。図12は、被監視側の管理プロトコルプロキシの構成である。

【0050】被監視側の管理プロトコルプロキシ60bは、監視側の管理プロトコルプロキシ60aとの間のプロキシ間通信経路70の確立および管理プロトコルプロキシデータの送受信を処理するプロキシ間通信部61と、管理プロトコルプロキシデータの分解組立を処理するプロキシデータ組立分解部62と、管理プロトコルのPDU内のアドレス情報をアドレス変換するアドレス変換処理部63と、アドレス変換処理部への入力となるASN.1MIB定義文64およびアドレス変換定義65と、被監視装置との間でSNMPメッセージを送受信するSNMPメッセージ送受信部66からなる。

【0051】監視装置40が発行した管理プロトコルのメッセージが監視側の管理プロトコルプロキシ60aによって管理プロトコルプロキシデータに変換されて、被監視側の管理プロトコルプロキシに送信されると、まずプロキシ間通信部61が送信された管理プロトコルプロキシデータを受信し、プロキシデータ組立分解部62に渡す。プロキシデータ組立分解部62は、受取った管理プロトコルプロキシデータを分解し、アドレス変換処理部63に渡す。アドレス変換処理部63は、ASN.1MIB定義文64およびアドレス変換定義65に従って、渡された管理プロトコルプロキシデータの送信元アドレスデータ、送信先アドレスデータ、さらに管理プロトコルのPDU中のアドレス情報をアドレス変換し、変換結

果をプロキシデータ分解組立部62に渡す。プロキシデータ組立分解部62は、プロキシデータの中から、送信先情報、送信元情報、管理プロトコルのPDUを取り出し、SNMPメッセージ送受信部66に渡す。SNMPメッセージ送受信部66は、送信先に指定された被監視装置50に対して、管理プロトコルのPDUを送信する。すなわちSNMPメッセージを送信する。被監視装置50は、送信されたSNMPメッセージに対応する応答をSNMPメッセージ送受信部66に返す。SNMPメッセージ送受信部66は、受信した応答のSNMPメッセージと、その送信元、送信先の情報をプロキシデータ組立分解部62に渡す。さらにプロキシデータ組立分解部62は、送信先、送信元、応答である管理プロトコルのPDUをアドレス変換処理部に渡す。アドレス変換処理部63は、ASN.1MIB定義文64およびアドレス変換定義65に従って、渡された管理プロトコルプロキシデータの送信元アドレスデータ、送信先アドレスデータ、さらに管理プロトコルのPDU中のアドレス情報をアドレス変換し、変換結果をプロキシデータ分解組立部62に渡す。さらにプロキシデータ分解組立部62は、送信先、送信元、管理プロトコルのPDUを管理プロトコルプロキシデータとして組み立てて、プロキシ間通信部61に渡す。プロキシ間通信部61は、管理プロトコルプロキシデータを監視側の管理プロトコルプロキシ60aへと送信し、監視側の管理プロトコルプロキシ60aが監視装置40へ管理プロトコルのPDUを返す。

【0052】ここで、ASN.1MIB定義文64は、RFC1212 (Concise MIB Definitions) などに記載されているMIBオブジェクトの標準的な記述方法であるところの、ASN.1 (Abstract Syntax Notation One=抽象構文記法.1) により記述されたMIB定義文である。一般に、ASN.1によるMIB定義文は、そのMIBモジュールを定義した者によって広く公開されている。本実施例では、ASN.1によるMIB定義文を解析して得られる情報を使用して管理プロトコルのプロトコルデータユニットのVariable-bindingsに含まれるアドレスを変換するため、特別な定義文が不要となり構成がより簡単となる。

【0053】図13は、監視側の管理プロトコルプロキシの構成である。監視側の管理プロトコルプロキシ60aは、監視装置40上のSNMP監視マネージャ41との間でSNMPメッセージを送受信するSNMPメッセージ送受信部66と、管理プロトコルプロキシデータの分解組立を処理するプロキシデータ組立分解部62と、被監視側の管理プロトコルプロキシ60bとの間のプロキシ間通信経路70の確立および管理プロトコルプロキシデータの送受信を処理するプロキシ間通信部61とからなる。監視装置40上のSNMP監視マネージャ41が発行したSNMPメッセージが監視側の管理プロトコルプロキシ60aに渡されると、SNMPメッセージ送受信部66がSNMPメッセージを受信し、それをプロ

キシデータ組立分解部62に渡す。プロキシデータ組立分解部62は、渡されたSNMPメッセージと、その送信先、送信元情報から、管理プロトコルプロキシデータを組み立てて、プロキシ間通信部61に渡す。プロキシ間通信部61は、渡された管理プロトコルプロキシデータを被監視側の管理プロトコルプロキシ60bに送信する。さらにプロキシ間通信部61は被管理側の管理プロトコルプロキシ60bから返される応答の管理プロトコルプロキシデータを受信して、プロキシデータ組立分解部62に渡す。プロキシデータ組立分解部62は、管理プロトコルプロキシデータから送信元、送信先、およびSNMPメッセージを取り出し、SNMPメッセージ送受信部66に渡す。SNMPメッセージ送受信部は渡された情報に従って、SNMPメッセージを監視装置40上のSNMP監視マネージャ41に返す。

【0054】図14は、管理側の管理プロトコルプロキシ60aと被管理側の管理プロトコルプロキシ60bとの間のプロキシ間通信経路70上で送受信される管理プロトコルプロキシデータの一例であり、管理プロトコルがSNMPである場合の例である。この場合、管理プロトコルプロキシデータは、SNMPメッセージの送信元、SNMPメッセージの送信先、SNMP PDUからなるデータである。

【0055】図2は、通常のSNMPメッセージのパケットの図である。パケットはネットワーク層であるところのIP層より上位の部分についてだけ示している。通常のSNMPパケットではIP層レベルでの送信元、送信先情報が、そのままSNMPメッセージ自体の送信元、送信先になっている。

【0056】図3は、管理プロトコルがSNMPである場合の管理プロトコルプロキシデータのパケットの図である。パケットはネットワーク層であるところのIP層より上位の部分についてだけ示している。管理プロトコルプロキシデータのパケットにおいては、IP層レベルでの送信元、送信先は、プロキシ間通信経路70の両端に存在する管理プロトコルプロキシのどちらかであり、SNMPメッセージの送信元、送信先のデータは、アプリケーション層に相当する管理プロトコルプロキシデータとしてパケットに含まれる。従って、アドレス変換のために使用する仮想的なアドレスは、実際の通信パケットの送信先または送信元アドレスとしては使用されない。このため、NICなどの機関から自組織に対して割り当てられていない仮想的なアドレスを使用したとしても、IP層すなわちネットワーク層レベルでの通信に何ら支障をきたすものではない。

【0057】このように管理プロトコルプロキシデータ上のSNMPメッセージ送信元、送信先アドレスをアドレス変換することにより、管理用アドレスに正式なグローバルアドレスではない仮想的なアドレスを使用することができ、グローバルアドレスを持たない装置まで含め

てプライベートネットワークをネットワーク管理することができる。

【0058】図15、図16、図17、図18を用いて、プロキシデータ組立分解部62を説明する。図15は、プロキシデータ組立分解部62の構成である。

【0059】プロキシデータ組立分解部62は、組立分解処理を実行する組立分解処理部68と、SNMPメッセージの送信先アドレスとそのSNMPメッセージを送信すべき相手プロキシとの対応付けを定義した相手プロキシ定義69からなる。

【0060】図16は、相手プロキシ定義の定義例である。定義行311は、送信先アドレスの第1オクテットが100であるSNMPメッセージは、アドレスが200.10.20.30の管理プロトコルプロキシへと送信することを表わす定義行である。

【0061】定義行312は、送信先アドレスの第1オクテットが101、第2オクテットが10であるSNMPメッセージは、アドレスが200.10.20.30の管理プロトコルプロキシへと送信することを表わす定義行である。

【0062】定義行313は、送信先アドレスの第1オクテットが110、第2オクテットが20、第3オクテットが80であるSNMPメッセージは、アドレスが230.51.62.72の管理プロトコルプロキシへと送信することを表わす定義行である。

【0063】定義行314は、送信先アドレスが120.60.11.8であるSNMPメッセージは、アドレスが230.51.62.72の管理プロトコルプロキシへと送信することを表わす定義行である。なお、このとき送信先アドレスは管理用アドレスを用いて表わす。

【0064】図17は、プロキシデータ組立処理のフローチャートである。ステップ151でSNMPメッセージ送受信部からSNMPメッセージを受取る。ステップ152でSNMPメッセージのIPヘッダ部から、送信元アドレスと送信先アドレスを取り出す。ステップ153でSNMPメッセージからSNMP PDUを取り出す。ステップ154で取り出した送信元アドレス、送信先アドレス、SNMP PDUを管理プロトコルプロキシデータに格納する。ステップ155で相手プロキシ定義中でSNMPメッセージのIPヘッダ部から取り出した送信先アドレスと対応づけられている相手プロキシアドレスを検索し、その相手プロキシアドレスをプロトコルプロキシデータの送信先と決定する。以上のようにしてプロキシデータ組立分解部は管理プロトコルプロキシデータを組み立てる。

【0065】図18は、プロキシデータ分解処理のフローチャートである。ステップ161でプロキシ間通信部から管理プロトコルプロキシデータと、その管理プロトコルプロキシデータを送信した相手である管理プロトコルプロキシのアドレスとを受取る。ステップ162で管理プロトコルプロキシデータから、送信元アドレス、送

信先アドレス、SNMP PDUを取り出す。ステップ163で取り出した送信元アドレスと送信先アドレスをSNMPメッセージのIPヘッダ部に格納する。ステップ164で取り出したSNMP PDUをSNMPメッセージに格納する。以上のようにしてプロキシデータ組立分解部は管理プロトコルプロキシデータを分解する。

【0066】図19は、アドレス変換処理部63の構成を表わす図である。アドレス変換処理部63は、SNMPメッセージの送信元と送信先のアドレスを変換するSNMPメッセージ送信元送信先アドレス変換部85と、SNMP PDU内に含まれるアドレス情報を変換するPDUアドレス変換部80からなる。さらにPDUアドレス変換部80は、PDUの解析とアドレス変換を処理するPDU解析変換部81と、PDUに含まれるアドレス情報のうちオブジェクト識別子として含まれるアドレスの変換を処理するオブジェクト識別子アドレス変換部82と、PDUに含まれるアドレス情報のうちMIB値として含まれるアドレスの変換を処理するMIB値アドレス変換部83と、PDUに含まれるアドレス情報のうちトラップ送信元アドレスとして含まれるアドレスの変換を処理するトラップ送信元アドレス変換部84とからなる。

【0067】プロキシデータ組立分解部62から、アドレス変換処理部63に管理プロトコルプロキシデータが渡されると、まずSNMPメッセージ送信元送信先アドレス変換部85が、アドレス変換定義65に従って、管理プロトコルプロキシデータ中のSNMPメッセージ送信元、送信先についてアドレス変換を行う。次にSNMPメッセージ送信元送信先アドレス変換部85は、管理プロトコルプロキシデータをPDU解析変換部81に渡す。PDU解析変換部81は、渡された管理プロトコルプロキシデータ中のPDUについて解析を実施し、その中からアドレス変換が必要な部分を抽出する。まず、PDUからトラップ送信元アドレス部分を抽出し、トラップ送信元アドレス変換部84に渡し、トラップ送信元アドレス変換部84は、アドレス変換定義65に従ってトラップ送信元アドレスをアドレス変換してPDU解析変換部81に返す。PDU解析変換部81は、トラップ送信元アドレス変換部84から受取った変換後のアドレスで、PDUのトラップ送信元アドレス部分を置き換える。さらに、PDUからデータの種別がIPアドレスを表わすものであるMIB値を抽出し、MIB値アドレス変換部83に渡し、MIB値アドレス変換部83は、アドレス変換定義65に従ってMIB値をアドレス変換してPDU解析変換部81に返す。PDU解析変換部81は、MIB値アドレス変換部83から受取った変換後のアドレスで、PDUのMIB値部分を置き換える。さらに、PDUからMIBのオブジェクト識別子を抽出し、オブジェクト識別子アドレス変換部82に渡し、オブジェクト識別子アドレス変換部82は、ASN.1 MIB

定義文とアドレス変換定義65とに従ってオブジェクト識別子の中に含まれるIPアドレスをアドレス変換してPDU解析変換部81に返す。PDU解析変換部81は、オブジェクト識別子アドレス変換部82から受取った変換後のアドレスで、PDUのMIBのオブジェクト識別子部分を置き換える。最後にPDU解析変換部はアドレス変換を行った後のPDUを含んだ管理プロトコルプロキシデータをプロキシデータ組立分解部62に返す。以上のようにしてアドレス変換処理部は管理プロトコルのデータについてアドレス変換を行うことができる。

【0068】図20は、オブジェクト識別子アドレス変換部82の構成である。オブジェクト識別子アドレス変換部82は、ASN.1 MIB定義文65を解釈するASN.1 MIB定義文解釈部88と、解釈したMIBの定義内容をもとにオブジェクト識別子を変換する必要があるオブジェクトを抽出する変換対象オブジェクト識別子抽出部89と、PDU解析変換部81から渡されたオブジェクト識別子と、変換対象オブジェクト識別子抽出部89が抽出したオブジェクト識別子とを比較して、渡されたオブジェクト識別子は変換が必要かどうかを判断するオブジェクト識別子比較部86と、変換対象オブジェクト識別子抽出部が抽出した定義情報とアドレス変換定義65とに基づいて、オブジェクト識別子をアドレス変換するアドレス変換実行部87とからなる。

【0069】まず、ASN.1 MIB定義文解釈部88がASN.1 MIB定義文65を読み込んで解釈し、解釈した結果得たMIB定義の情報を変換対象オブジェクト識別子抽出部89に渡す。変換対象オブジェクト識別子抽出部89は、渡されたMIB定義の中からオブジェクト識別子にIPアドレスを含む可能性があるMIBオブジェクトを抽出し、該当するMIBオブジェクトのオブジェクト識別子の一覧をオブジェクト識別子比較部86へ、該当するMIBオブジェクトの定義情報であるところのINDEX情報をアドレス変換実行部87へそれぞれ渡す。ここで、オブジェクト識別子にIPアドレスを含む可能性があるMIBオブジェクトとは、MIBテーブルを表わすMIBオブジェクトであり、テーブルのINDEXとして使用するMIBテーブル内MIBオブジェクトのうちの1つ以上がIPアドレスであるようなMIBオブジェクトである。このようなオブジェクトは、MIBオブジェクトの値であるところのインスタンスをGETリクエストなどで取得する際にMIBオブジェクトのオブジェクト識別子に続けてインスタンス識別子であるところのINDEXを付加して1つのオブジェクト識別子として指定するが、このときのINDEXにIPアドレスが使用されるため、オブジェクト識別子にIPアドレスが含まれる可能性があるものである。また、アドレス変換実行部87へ渡すINDEX情報としては、MIBテーブルのINDEXとして複数のMIB

オブジェクトが対応づけられているときに、その中の I P アドレスの部分だけを変換するために、INDEX として使われる M I B オブジェクトの種別であるところの SYNTAX を順に並べた情報を渡す。例えば、INDEX として整数の M I B オブジェクト 1 つと I P アドレスを取るような M I B テーブルの場合、インスタンス識別子は、整数の分の 1 つと I P アドレスの分 4 つの合計 5 つの副識別子を持つ識別子となる。アドレス変換では、このうちの 2 番目から 5 番目の副識別子を I P アドレスと解釈して変換する必要があるため、アドレス変換実行部 87 へ INDEX は、整数 1 つと I P アドレス 1 つの組であるという情報を渡す必要がある。

【0070】さてここで、PDU 解析変換部 81 から PDU 中のオブジェクト識別子がオブジェクト識別子アドレス変換部 82 に渡されると、まずオブジェクト識別子比較部 86 がオブジェクト識別子を受取る。オブジェクト識別子比較部 86 は、PDU 解析変換部 81 から渡されたオブジェクト識別子と、変換対象オブジェクト識別子抽出部 89 が抽出した変換対象のオブジェクト識別子一覧とを比較し、PDU 解析変換部 81 から渡されたオブジェクト識別子が変換対象のオブジェクト識別子一覧に含まれていたなら、PDU 解析変換部 81 からオブジェクト識別子をアドレス変換実行部 87 に渡す。PDU 解析変換部 81 から渡されたオブジェクト識別子が変換対象のオブジェクト識別子一覧に含まれていなかったら、PDU 解析変換部 81 から渡されたオブジェクト識別子を何も変換せずにそのまま PDU 解析変換部 81 へ返す。

【0071】次に、アドレス変換実行部 87 は渡されたオブジェクト識別子について、まず変換対象オブジェクト抽出部 89 から渡された INDEX 情報に基づいてオブジェクト識別子中に現れる I P アドレスの位置、すなわち変換位置を特定し、次にアドレス変換定義 65 に基づいてアドレス変換を実行し、変換後のオブジェクト識別子を PDU 解析変換部 81 へ返す。

【0072】以上のようにしてオブジェクト識別子アドレス変換部は、M I B のオブジェクト識別子に含まれる I P アドレスをアドレス変換することができる。

【0073】図 21 のフローチャートを用いて PDU 解析変換部の処理を説明する。ステップ 111 で PDU から PDU 種別を表わすデータを抽出する。ステップ 112 で PDU 種別からアドレス変換方向を決定する。アドレス変換方向とは、PDU 中のアドレスを、管理用アドレスから実アドレスに変換するのか、実アドレスから管理用アドレスに変換するのか、ということの意味する。監視側から被監視側へ送信される PDU は、管理用アドレスを実アドレスに変換する。被監視側から監視側へ送信される PDU は、実アドレスを管理用アドレスに変換する。監視側から被監視側へ送信されるのか、被監視側から監視側へ送信されるのかは、PDU 種別毎に決まっているため、図 2

2 の表に従って PDU 種別からアドレス変換方向を決定することができる。ステップ 113 で PDU の種別が SNMP トラップであるかどうか判定する。SNMP トラップの場合は、ステップ 114 に進む。SNMP トラップでない場合は、ステップ 117 に進む。ステップ 114 で、PDU からトラップ送信元アドレスを抽出する。ステップ 115 で、トラップ送信元アドレス変換部にステップ 114 で抽出したトラップ送信元アドレスと、ステップ 112 で決定したアドレス変換方向の情報とを渡し、変換後のトラップ送信元アドレスを受取る。ステップ 116 で、PDU のトラップ送信元アドレスを、ステップ 115 で受取った変換後のトラップ送信元アドレスに置き換える。ステップ 117 で、PDU 中に variableBindingList が存在するかどうかを判定する。variableBindingList が存在する場合、ステップ 118 に進む。variableBindingList が存在しない場合、PDU 解析変換部の処理を終了する。ステップ 118 で、variableBindingList からまだ処理していない variableBind を 1 つ抽出する。ステップ 119 で、ステップ 118 で抽出した variableBind からオブジェクト識別子と値を抽出する。ステップ 120 で、M I B 値アドレス変換部に、ステップ 119 で抽出した M I B 値と、ステップ 112 で決定した変換方向の情報とを渡し、変換後の M I B 値を受取る。ステップ 121 で、オブジェクト識別子アドレス変換部に、ステップ 119 で抽出したオブジェクト識別子と、ステップ 112 で決定した変換方向の情報とを渡し、変換後のオブジェクト識別子を受取る。ステップ 122 で、PDU の variableBind のオブジェクト識別子をステップ 121 で受取った変換後のオブジェクト識別子に、variableBind の M I B 値をステップ 120 で受取った変換後の M I B 値に、それぞれ置き換える。ステップ 123 で、未処理の variableBinding がまだ残っているかどうかを判定する。残っているならばステップ 118 へ進む。残っていないならば、PDU 解析変換部の処理を終了する。以上のようにして、PDU 中のアドレス情報を変換することができる。図 23 のフローチャートを用いて変換対象オブジェクト識別子抽出部の処理を説明する。

【0074】ステップ 131 で、M I B 定義文に定義されているオブジェクト識別子を 1 つ取り出す。ステップ 132 で、ステップ 131 において取り出したオブジェクト識別子が M I B テーブルを表わす識別子かどうかを判定する。M I B テーブルを表わす識別子の場合は、ステップ 133 に進む。M I B テーブルを表わす識別子でない場合は、ステップ 136 に進む。ステップ 133 で、オブジェクト識別子の INDEX として指定されているテーブル内 M I B オブジェクトの SYNTAX を抽出する。ステップ 134 で、ステップ 133 において抽出したテーブル内 M I B オブジェクトの SYNTAX が I P アドレスを表わす SYNTAX であるようなものか一つでもあるかどうかを判定する。ある場合は、ステッ

ブ135へ進む。ない場合は、ステップ136へ進む。
ステップ135で、ステップ131において取り出した
オブジェクト識別子は、変換対象のオブジェクト識別子
であると判断する。

【0075】ステップ136で、ステップ131におい
て取り出したオブジェクト識別子は、変換対象のオブ
ジェクト識別子ではないと判断する。ステップ137で、
MIB定義文の中に、未処理のオブジェクト識別子がま
だあるかどうかを判定する。まだある場合は、ステッ
プ131に進む。ない場合は、ステップ138に進む。ス
テップ138で、変換対象と判断したオブジェクト識別
子を全てオブジェクト識別子比較部へ通知する。ステッ
プ139で、変換対象と判断したオブジェクト識別子の
INDEX情報を全てアドレス変換実行部へ通知する。
以上のようにして、変換対象オブジェクト識別子抽出部
の処理を実現することができる。

【0076】図24は、アドレス変換定義65の定義例
である。定義行301は、IPアドレスの第1オクテット
のみを変換する場合の定義例である。この場合、第1オ
クテットが10である実アドレスは全て第1オクテットを1
00に変換したものが管理用アドレスとなる。例えば、監
視装置40から送信された管理プロトコルのデータ中に
アドレス100.1.2.3があった場合、そのアドレスはアド
レス変換によって10.1.2.3に変換されて被監視装置50
へ中継される。反対に、被監視装置50からの応答中に
アドレス10.1.2.3があった場合は、そのアドレスはアド
レス変換によって100.1.2.3に変換されて監視装置40
へ中継される。定義行302は、IPアドレスの第1オク
テットと第2オクテットを変換する場合の定義例であ
る。この場合、第1オクテットが172であり、第2オク
テットが16である実アドレスは全て第1オクテットを101
に変換し、第2オクテットを10に変換したものが管理用
アドレスとなる。例えば、監視装置40から送信された
管理プロトコルのデータ中にアドレス101.10.1.2があ
った場合、そのアドレスはアドレス変換によって172.16.
1.2に変換されて被監視装置50へ中継される。反対
に、被監視装置50からの応答中にアドレス172.16.1.2
があった場合は、そのアドレスはアドレス変換によって
101.10.1.2に変換されて監視装置40へ中継される。定
義行303は、IPアドレスの第1オクテットと第2オク
テットと第3オクテットを変換する場合の定義例であ
る。この場合、第1オクテットが172であり、第2オク
テットが17であり、第3オクテットが50である実アド
レスは全て第1オクテットを110に変換し、第2オクテ
ットを20に変換し、第3オクテットを80に変換したもの
が管理用アドレスとなる。例えば、監視装置40から送信
された管理プロトコルのデータ中にアドレス110.20.80.1
があった場合、そのアドレスはアドレス変換によって17
2.17.50.1に変換されて被監視装置50へ中継される。
反対に、被監視装置50からの応答中にアドレス172.1

7.50.1があった場合は、そのアドレスはアドレス変換に
よって110.20.80.1に変換されて監視装置40へ中継さ
れる。定義行304は、IPアドレスの第1オクテットか
ら第4オクテットの全てのオクテットを変換する場合の
定義例である。この場合、アドレスが192.168.20.5であ
る実アドレスは、管理用アドレス120.60.11.8に変換さ
れる。例えば、監視装置40から送信された管理プロト
コルのデータ中にアドレス120.60.11.8があった場合、
そのアドレスはアドレス変換によって192.168.20.5に変
換されて被監視装置50へ中継される。反対に、被監視
装置50からの応答中にアドレス192.168.20.5があった
場合は、そのアドレスはアドレス変換によって120.60.1
1.8に変換されて監視装置40へ中継される。

【0077】図25は、別の仮想的ネットワーク管理シ
ステムの構成例である。この場合、監視装置40および
監視装置側の管理プロトコルプロキシ60aは、グロー
バルネットワーク10上に存在するが、図1の構成の場
合と何ら変わりにく管理用アドレスを用いた仮想的なネ
ットワーク管理を行うことが可能である。

【0078】図26および図27は、さらに別の実施例
における管理プロトコルプロキシの構成であり、監視側
の管理プロトコルプロキシでアドレス変換する場合の実
施例である。

【0079】この場合も、図12および図13に示した
被監視側の管理プロトコルプロキシでアドレス変換する
場合と同様の方法でアドレス変換を実行することができ
る。ただし、監視側の管理プロトコルプロキシにおいて
アドレス変換する場合は、監視側の管理プロトコルプロ
キシに定義するアドレス変換定義は、被監視側のプライ
ベートネットワークごとに別々に定義し、例えば被監視
側のプライベートネットワークB用にアドレス変換定義
65bを、被監視側のプライベートネットワークC用に
アドレス変換定義65cを、それぞれ定義するようにす
る。これにより図9の構成のように複数の被監視側プ
ライベートネットワークにおいて監視装置のプライベート
アドレスが競合しているような場合でも、正しくアドレ
ス変換できるようにする。

【0080】図28および図29は、また別の実施例に
おける仮想ネットワーク管理システムの構成と、被管理
側の管理プロトコルプロキシの構成であり、被管理側の
管理プロトコルプロキシがRFC1631に準拠したN
ATと同一の装置上で動作するような構成である。

【0081】この例は、監視装置40と監視側の管理プ
ロトコルプロキシ60aは、グローバルネットワーク1
0上に存在し、アドレス変換は被監視側の管理プロトコ
ルプロキシで行い、被管理側の管理プロトコルプロキシ
がRFC1631に準拠したNAT20と同一の装置上
で動作するような構成である。

【0082】図29は、RFC1631に準拠した管理
プロトコルのアドレス変換機能を持たないNAT20と

同一の装置上で動作する被監視側の管理プロトコルプロキシ60bの構成である。プロキシ間通信部61が監視側の管理プロトコルプロキシ60aと通信するときに、NAT20のグローバルネットワーク側通信プロトコル処理部21を介して通信することと、SNMPメッセージ送受信部66が被監視装置50とデータを送受信するときに、NAT20のプライベートネットワーク側通信プロトコル処理部23を介して通信することとが、図12の構成との違いである。なお、NAT20のRFC1631に準拠した動きとして、NAT20の装置をグローバルネットワーク側からプライベートネットワーク側へ通り抜けようとするパケットについては、まずグローバルネットワーク側通信プロトコル処理部21が通り抜けようとするパケットを捕らえてRFC1631準拠アドレス変換処理部22へ渡し、RFC1631準拠アドレス変換処理部22がアドレス変換をした後、プライベートネットワーク側通信プロトコル処理部23へパケットを渡し、プライベートネットワーク側通信プロトコル処理部23によってプライベートネットワーク側へ送出される。

【0083】反対に、プライベートネットワーク側からグローバルネットワーク側へ通り抜けようとするパケットについては、まずプライベートネットワーク側通信プロトコル処理部23が通り抜けようとするパケットを捕らえてRFC1631準拠アドレス変換処理部22へ渡し、RFC1631準拠アドレス変換処理部22がアドレス変換をした後、グローバルネットワーク側通信プロトコル処理部21へパケットを渡し、グローバルネットワーク側通信プロトコル処理部21によってグローバルネットワーク側へ送出される。

【0084】しかしながら、プロキシ間通信部61による通信は、NATおよび被監視側の管理プロトコルプロキシが動作する装置のグローバルネットワーク側のアドレスを送信先または送信元とする通信であり、NAT20を通り抜けようとする通信ではない。このため、RFC1631準拠アドレス変換処理部22は通らずに、グローバルネットワーク側通信処理部21からプロキシ間通信部61へデータがそのまま渡される。

【0085】また、SNMPメッセージ送受信部66による通信についても、NATおよび被監視側の管理プロトコルプロキシが動作する装置のプライベートネットワーク側のアドレスを送信先または送信元とする通信であり、NAT20を通り抜けようとする通信ではない。このため、RFC1631準拠アドレス変換処理部22は通らずに、プライベートネットワーク側通信処理部23からSNMPメッセージ送受信部66へデータがそのまま渡される。

【0086】以上のことから、図12に示した被監視側の管理プロトコルプロキシと同じ構成の管理プロトコルプロキシを用いて、NAT20と同一の装置上で動作さ

て仮想的なネットワーク管理を実現することが可能である。

【0087】尚、既に述べたとおり管理プロトコルプロキシの処理はフローチャートで示したとおり、プログラムによって実現することができる。

【0088】以上、NATがIP層のアドレス変換を行うものとして説明したが（NATが管理プロトコルのPDU部分のアドレスを変換する機能有していない。）、NATがIP層のアドレス変換を行う機能と、管理プロトコルのPDU部分のアドレスを変換する機能を有している場合には、NATと管理プロトコルプロキシサーバとを選択的に利用して、管理プロトコルのPDU部分のアドレス変換を行うことができる。

【0089】

【発明の効果】以上説明したように、管理プロトコルのプロキシ間でデータ通信を行うことができ、グローバルアドレスを持たないノード間で管理プロトコルによるデータ通信を行うことができる。

【図面の簡単な説明】

【図1】ネットワークシステムの基本構成を示した図である。

【図2】SNMPメッセージのパケットの構成を示した図である。

【図3】管理プロトコルプロキシデータのパケットの構成を示した図である。

【図4】NATの機能を説明するための図である。

【図5】SNMPメッセージのパケットの構成を示した図である。

【図6】SNMPメッセージのパケットの構成を示した図である。

【図7】仮想ネットワーク管理システムにおける一適用例を示した図である。

【図8】仮想ネットワーク管理システムにおける一適用例を示した図である。

【図9】仮想ネットワーク管理システムにおける一適用例を示した図である。

【図10】仮想ネットワーク管理システムにおける一適用例を示した図である。

【図11】仮想ネットワーク管理システムにおける一適用例を示した図である。

【図12】被監視側の管理プロトコルプロキシの構成を示した図である。

【図13】監視側の管理プロトコルプロキシの構成を示した図である。

【図14】管理プロトコルプロキシデータの一例を示した図である。

【図15】プロキシデータ分解組立部の構成を示した図である。

【図16】相手プロキシ定義の定義例を示した図である。

【図17】プロキシデータ組立処理のフローチャートを示した図である。

【図18】プロキシデータ分解処理のフローチャートを示した図である。

【図19】アドレス変換処理部の構成を示した図である。

【図20】オブジェクト識別子アドレス変換部の構成を示した図である。

【図21】PDU解析変換部の処理のフローチャートを示した図である。

【図22】PDU種別とPDUの送信方向およびアドレス変換の変換方向との関係を表わした図である。

【図23】変換対象オブジェクト識別子抽出部の処理のフローチャートを示した図である。

【図24】アドレス変換定義の定義例を示した図である。

【図25】仮想ネットワーク管理システムの構成例を示した図である。

【図26】管理プロトコルプロキシの構成を示した図である。

【図27】管理プロトコルプロキシの構成を示した図である。

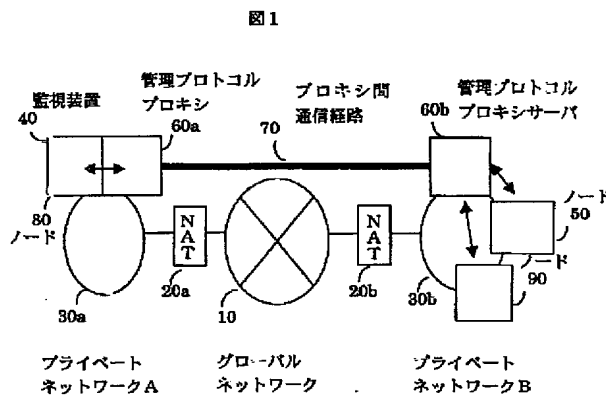
【図28】仮想ネットワーク管理システムの構成を示した図である。

【図29】被管理側の管理プロトコルプロキシの構成を示した図である。

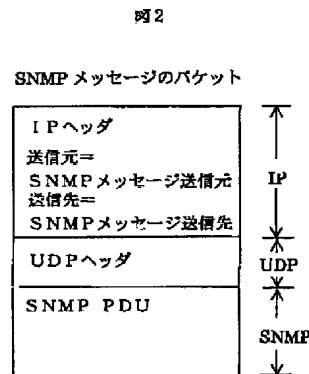
【符号の説明】

10…グローバルネットワーク、20…NAT、30…プライベートネットワーク、40…監視装置、50…被監視装置、60…管理プロトコルプロキシ、70…プロキシ間通信経路

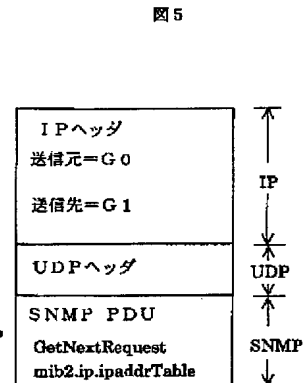
【図1】



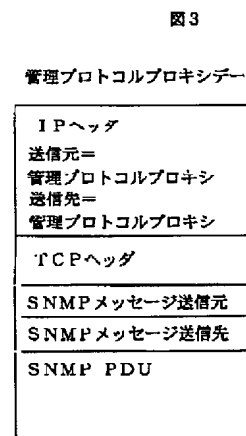
【図2】



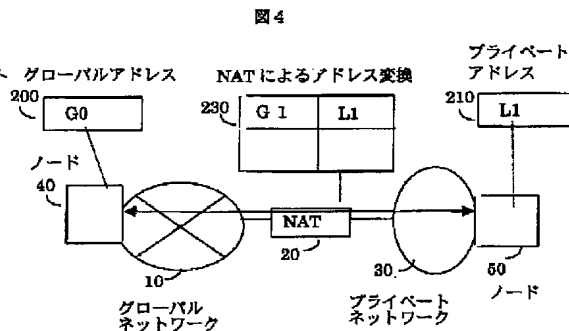
【図5】



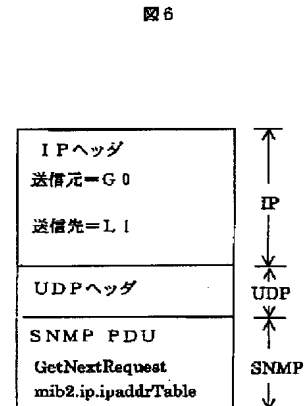
【図3】



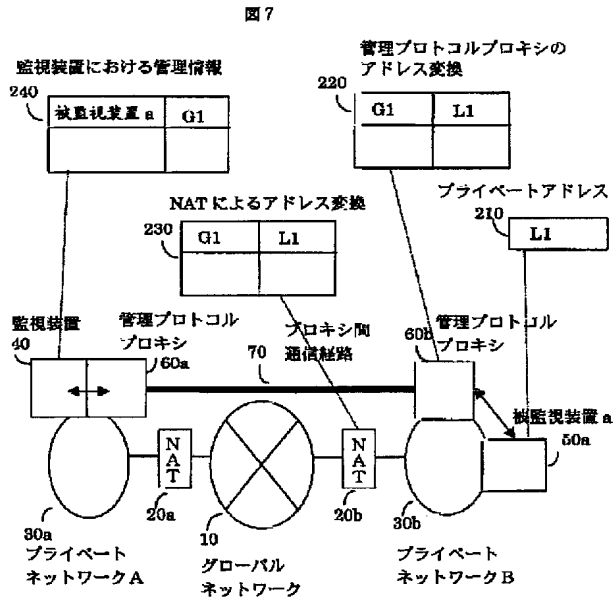
【図4】



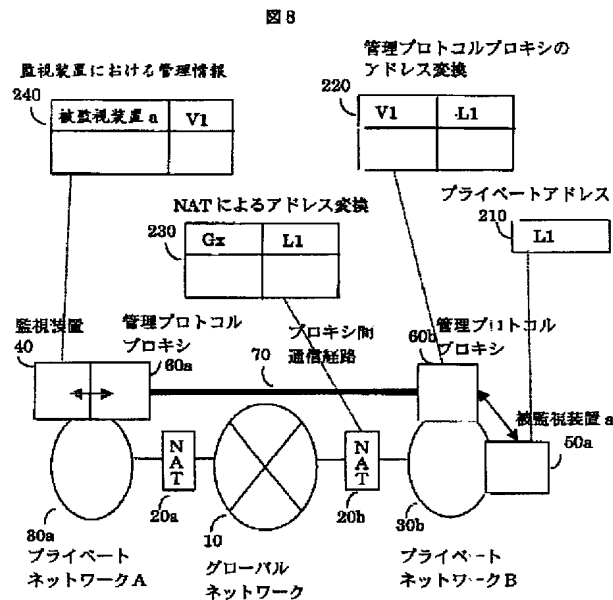
【図6】



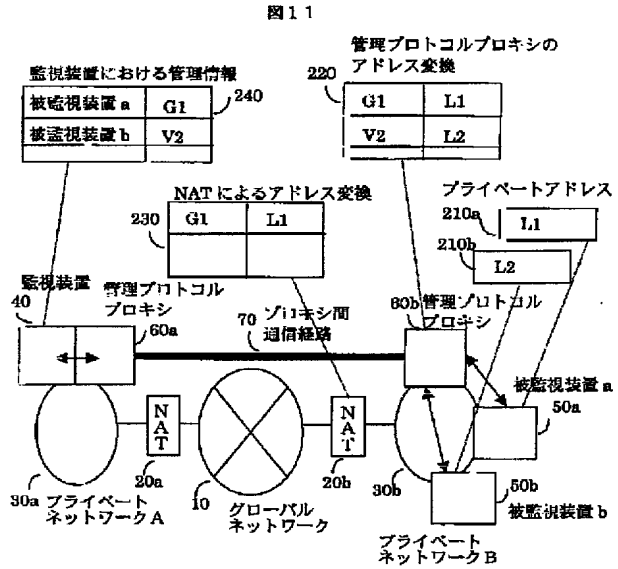
【図7】



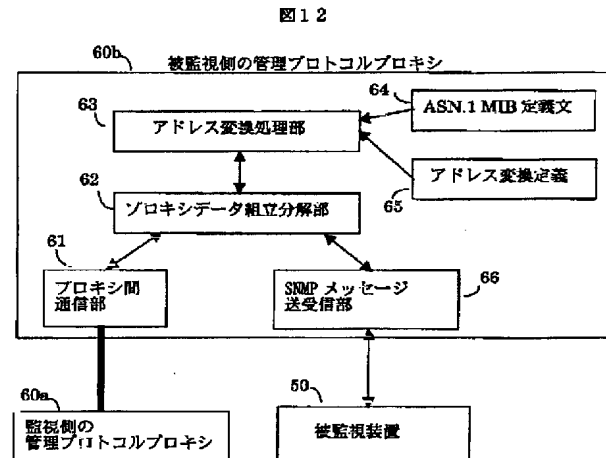
【図8】



【図11】



【図12】

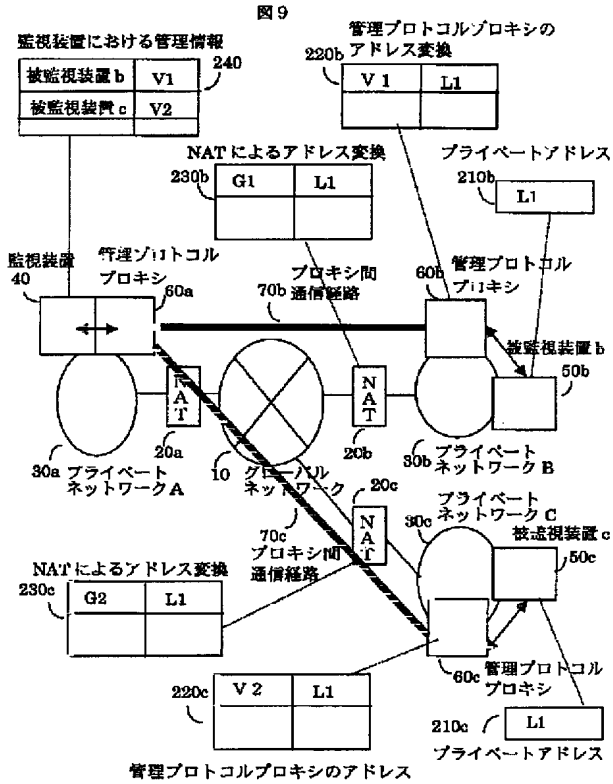


【図14】

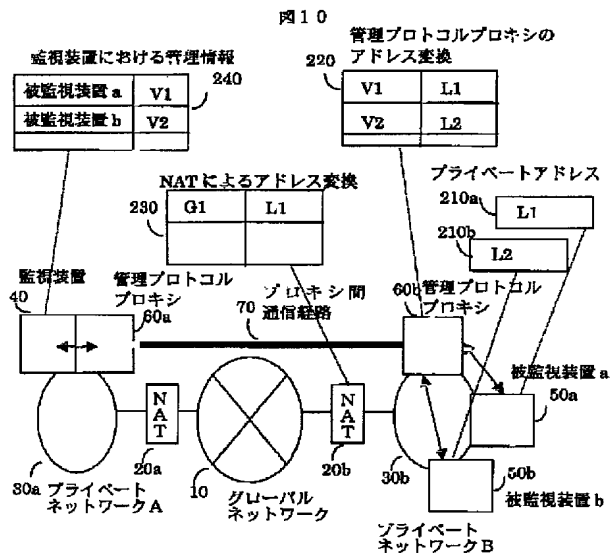
図14

SNMPメッセージ送信元
SNMPメッセージ送信先
SNMP PDU

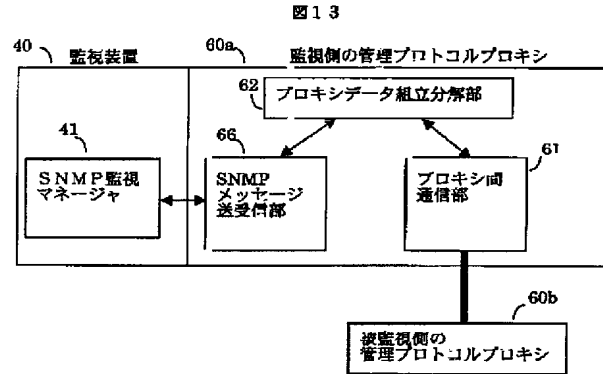
【図9】



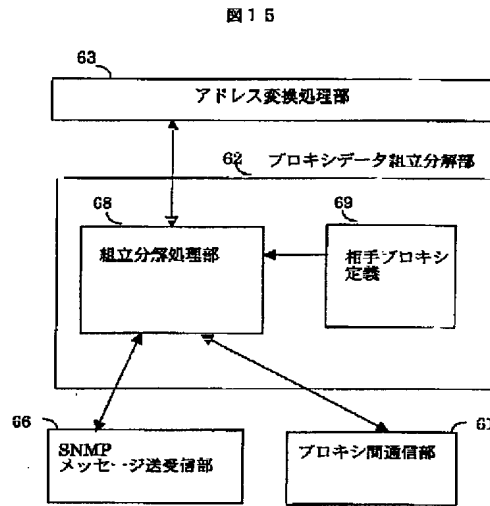
【図10】



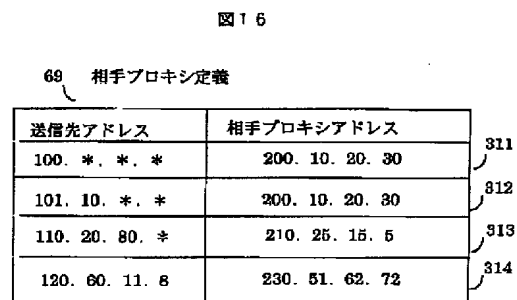
【図13】



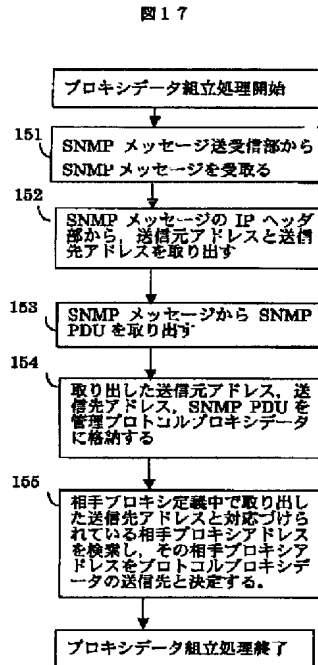
【図15】



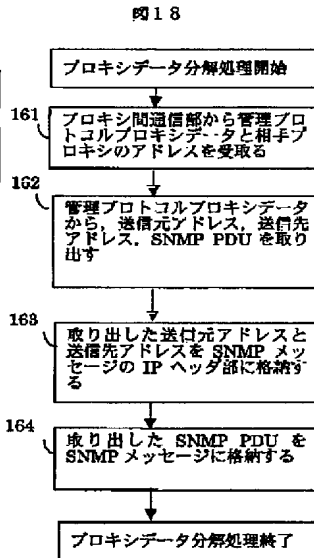
【図16】



【図17】



【図18】



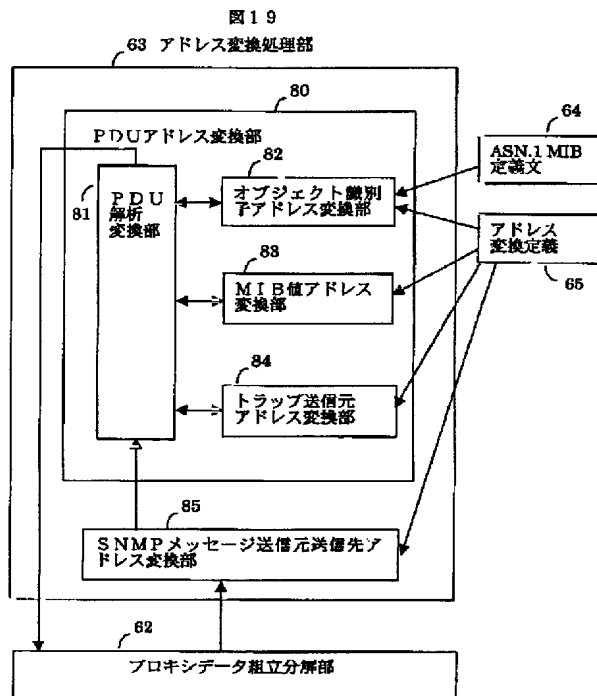
【図24】

図24

65 アドレス変換定義

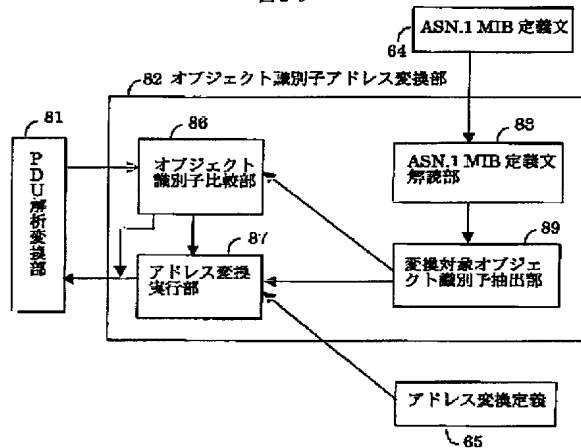
管理用アドレス	実アドレス
100. *. *. *	10. *. *. *
101. 10. *. *	172. 16. *. *
110. 20. 80. *	172. 17. 60. *
120. 60. 11. 8	192. 168. 20. 5

【図19】



【図20】

図20

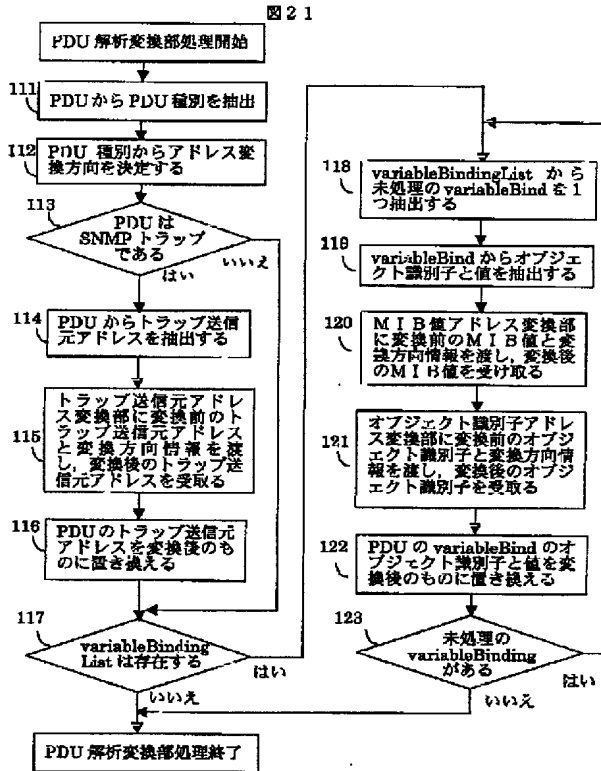


【図22】

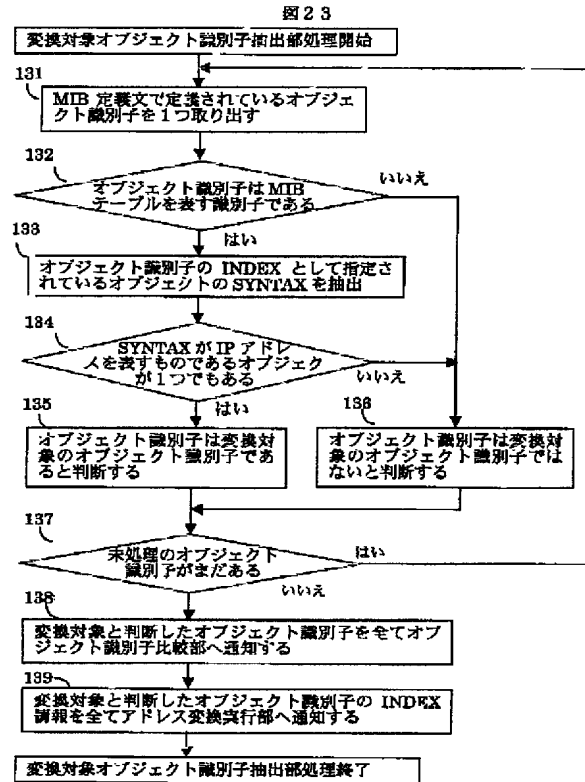
図22

送信方向	変換方向	PDU種別
監視装置側から被監視装置側へ送信	実アドレスから管理用アドレスへ変換	Get-Request, Getnext-Request, Set-Request
被監視装置側から監視装置側へ送信	実アドレスから管理用アドレスへ変換	Get-Response, Trap

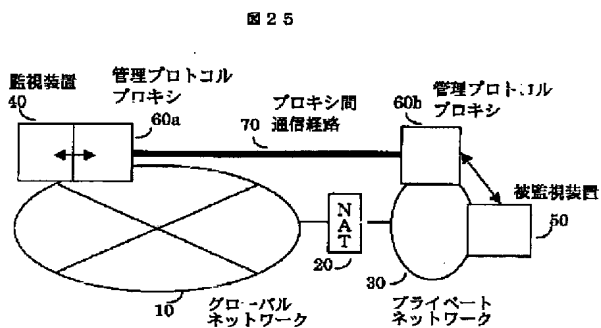
【図21】



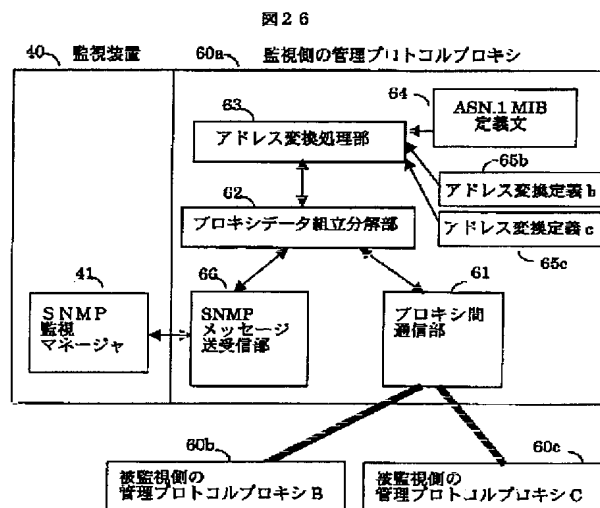
【図23】



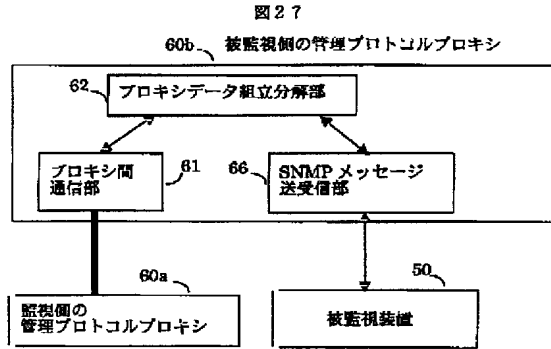
【図25】



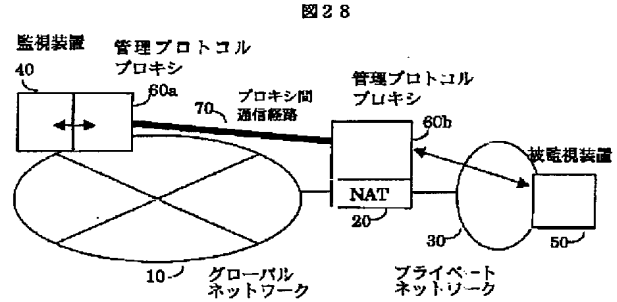
【図26】



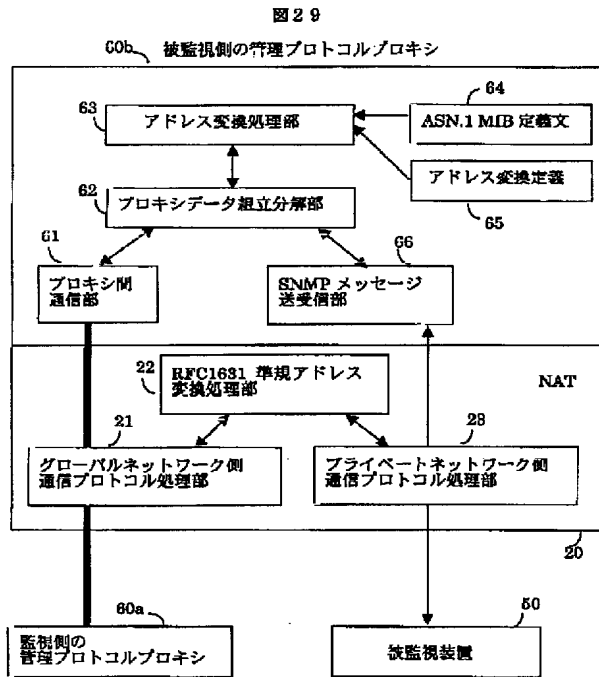
【図27】



【図28】



【図29】



JP 2002-190810 A

(11)Publication number : 2002-190810 (51)Int.Cl. H04L 12/28
(43)Date of publication of application : 05.07.2002
(21)Application number : 2000-393280 (71)Applicant :HITACHI LTD
(22)Date of filing : 21.12.2000 (72)Inventor : SHIBATA JUNJI

(54) NETWORK MANAGEMENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To allow data communication between nodes having no global address.

SOLUTION: The network management system manages a network system where a 1st network and a 2nd network adopting different address systems are connected via an address converter. The 1st and 2nd networks respectively have nodes and management protocol proxies and each management protocol proxy has a management protocol proxy data generating section that uses a sender address, a destination address, and a protocol data unit included in a packet in compliance with a management protocol sent from the node for management protocol proxy data and with an address conversion section that converts address information in the protocol data unit included in the management protocol proxy data sent from other management protocol proxy.

Disclaimer

This is a machine translation performed by INPIT (<http://www.ipdl.inpit.go.jp>) and received and compiled with PatBot (<http://www.patbot.de>). PatBot can't make any guarantees that this translation is received and displayed completely!

Notices from INPIT

Copyright (C) JPO, INPIT

The JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] A network management system which manages a network system to which the 1st network that differs in an addressing architecture, and the 2nd network were connected via an address conversion device, comprising:

Have said 1st and 2nd network, respectively and a node and a management protocol proxy said each management protocol proxy, A management protocol proxy data generating part used as management protocol proxy data which uses as data a transmission source address, a transmission destination address, and a Protocol Data Unit which are contained in a packet of a management protocol sent from a node.

An address conversion section which changes address information in a Protocol Data Unit contained in management protocol proxy data sent from other management protocol proxies.

[Claim 2] Said management protocol proxy has the address defining information which matched and carried out a transmission destination address included in a packet of a management protocol sent from a node, and an address of a management protocol proxy, The network management system according to claim 1 which determines an address of a management protocol proxy of a transmission destination from a transmission destination address to which said management protocol proxy data generating part has been sent from a node, and said address defining information.

[Claim 3] Address defining information which said management protocol proxy of at least one network of said 1st or 2nd network has, The network management system according to claim 1 defined by an address which is not defined by said address conversion device and an address of a management protocol proxy matching.

[Claim 4] A proxy of said management protocol has the address translation rule which defined address translation information, and said address conversion section, The network management system according to claim 2 which changes address information contained in a Protocol Data Unit of a management protocol by ASN.1 definition statement of an MIB object which is said address translation rule and the target of conversion.

[Claim 5] A network management system with which several networks with which addressing architectures differ manage a network system connected with an address conversion device, comprising:

Have two or more node and two or more management protocol proxies which were connected to each network, and said each management protocol proxy, A transmission source address and a transmission destination address which are included in a packet of a management protocol sent from a node, a management protocol proxy data generating part which uses data in a Protocol Data Unit as proxy data of a management protocol.

An address conversion section which changes address information in a Protocol Data Unit contained in proxy data of a management protocol sent from other management protocol proxies.

[Claim 6] It is a disposal method of a management protocol which processes a packet sent from a node and transmits, A transmission source address included in a packet of a management protocol sent from a node, A disposal method of a management protocol which changes address information in a Protocol Data Unit contained in proxy data of a management protocol which used data in a transmission destination address and a Protocol Data Unit as proxy data of a management protocol, and has been sent from other management protocol proxies.

[Claim 7] It is the storage with which processing of a management protocol which processes a packet of a management protocol sent from a node, and transmits was memorized and in which computer reading is possible, A transmission source address included in a packet of a management protocol sent from a node, Data in a transmission destination address and a Protocol Data Unit is used as proxy data of a management protocol, A storage with which processing which changes address information in a Protocol Data Unit contained in proxy data of a management protocol sent from a proxy of other management protocols was memorized and in which computer reading is possible.

[Claim 8] It is a program which processes a management protocol which processes a packet of a management protocol sent from a node, and transmits, A transmission source address included in a packet of a management protocol sent from a node, A program which changes address information in a Protocol Data Unit contained in proxy data of a management protocol which used data in a transmission destination address and a Protocol Data Unit as proxy data of a management protocol, and has been sent from a proxy of other management protocols.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a network management system, and relates to the network management system which manages the network system to which several networks with which addressing architectures differ mutually especially were connected.

[0002]

[Description of the Prior Art] Now, the IP address which is a network address most widely used on the Internet etc. is an address which is prescribed by the protocol called IPv4 (Internet Protocol ver.4) and has a 32-bit address space. The network address must be assigned at a meaning to the apparatus connected to a network, and assignment has been performed so that it may become a meaning with the organization etc. which are called NIC about the network address of the apparatus linked to the Internet. In IPv4, since it has a 32-bit address space, a piece, i.e., the address of 4 billion, can be assigned the 32nd power of 2 at the maximum theoretically. However, if the apparatus linked to the Internet increases, it will become difficult to assign the IP address of IPv4 to all the apparatus linked to the Internet.

[0003] The address conversion function it is indicated to be to RFC1631 (The IP Network Address Translator) which IETF defines to be widely used as art for solving this problem, It is the method which combined the private network indicated to RFC1918 (Address Allocation for Private Internets). This method is premised on all the apparatus that exists, for example in a network with a local network in a company, etc. not connecting with the network of the exteriors, such as the Internet. That is, first, the network with a local network in a company, etc. assigns an IP address using the address of the range of the private address indicated to RFC1918, and builds a network. It is made not to connect with external networks, such as the Internet, at this private address at this time. About the apparatus linked to external networks, such as the Internet. Between a local network and external networks, such as the Internet, Connection is made possible by arranging the address conversion device indicated to RFC1613, and changing into the global address for accessing the address of a transceiver packet from a private address by address translation at the Internet. A global address is an address assigned by NIC etc. here. At this time, a global address is assigned dynamically and a device which utilizes effectively a limited global address -- two or more local nodes enable it for a timetable to share one global address etc. -- is also performed.

[0004]By the way, in the address translation indicated in RFC1631, rewriting of the IP address of the transmitting origin included in the header of an IP packet and a transmission destination and change of the checksum of the IP header produced in connection with it are re-calculated and replaced. Communication by TCP/IP is attained by this and communication by the protocol of the upper layer is also attained.

[0005]However, although the IP address is included, for example in network management protocols, such as SNMP, also in the Protocol Data Unit (PDU) exchanged by a management protocol, Address translation of this portion is not carried out in the address conversion device indicated to RFC1631.

[0006]On the other hand, in addition to the function of the address translation indicated to RFC1631, to JP,11-187058,A, an address conversion device which carries out address translation also about the Protocol Data Unit of a management protocol is indicated.

[0007]

[Problem(s) to be Solved by the Invention]However, it will be performed by communication of the management protocol using the global address which can be used in the network by the side of a controlling device when an address conversion device performs employment by the private address and a global address. For this reason, communication by a management protocol can be performed only to the node to which it is in a supervising side and the global address is assigned. However, in network management, if manageable also about a node without such a global address, it will become possible to perform more effective management. In the method of JP,11-187058,A, it is not indicated about this point.

[0008]The purpose of this invention is to provide the network management system which can perform the data communications by a management protocol also between the nodes in which the network of a different addressing architecture does not have a global address in the network system connected by the address conversion device.

[0009]

[Means for Solving the Problem]As a way stage which attains the above-mentioned purpose, the 1st network that differs in an addressing architecture, and the 2nd network are the network management systems which manage a network system connected via an address conversion device, and the 1st and 2nd network is provided with the following.

Have a node and a management protocol proxy, respectively, and each management protocol proxy, A management protocol proxy data generating part used as management protocol proxy data which uses as data a transmission source address, a transmission destination address, and a Protocol Data Unit which are contained in a packet of a management protocol sent from a node.

An address conversion section which changes address information in a Protocol Data Unit contained in management protocol proxy data sent from other management protocol proxies.

[0010]Thereby, data communications can be performed between proxies of a management protocol, and data communications can be performed between nodes without a global address.

[0011]

[Embodiment of the Invention]Hereafter, the example at the time of applying SNMP to a management protocol according to a drawing is described. Drawing 1 shows the concept of the network management system explained by this example.

[0012]This system The global network 10, the private network A30a, NAT20a which has the private network B30b and performs address translation for the private network A30a and the global network 10, The private network B30b and the global network 10 are connected by NAT20b which performs address translation.

[0013]The node 80 for supervising is connected to the private network A30a. This

node 80 has the management protocol proxy 60a which performs generation of the monitoring instrument 40 which performs processing for supervising a monitored device, and the proxy data of a management protocol, address translation in the Protocol Data Unit contained in proxy data, etc.

[0014]The management protocol proxy server 60b which performs generation of the nodes 50 and 90 which are monitored devices, and the proxy data of a management protocol, address translation in the Protocol Data Unit contained in proxy data, etc. is connected to the private network B30b.

[0015]In such composition, the node 80 for this network management system to supervise manages the nodes 50 and 90 which are monitored devices.

[0016]When the monitoring instrument 40 of the node 80 of the private network A30a performs the node 50 and data communications which are monitored devices, It is made to perform data communications between the management protocol proxy 60a of the node 80, and the management protocol proxy server 60b of the private network B30b. This becomes equivalent to having formed the communication path 70 between proxies, and the virtual communication path to call.

[0017]If it does in this way, when the address used in the private network A30a differs from the address used in the private network B30b that is, data communications can be performed between the networks of a different addressing architecture. Data communications can be made possible even when the firewall etc. which pass neither the address of a private network nor the address of global network are formed between the private network A30a and the private network B30b.

[0018]Operation of the whole network system more concretely shown in drawing 1 is explained. Drawing 2 shows the SNMP message packet of management protocol SNMP of a node. Drawing 3 shows the packet of the management protocol proxy data of a management protocol proxy server. From the packet of management protocol SNMP transmitted from the node 50 which are the monitoring instrument 40 of the node 80, and a monitored device, and the node 90 to namely, the management protocol proxy 60a. As for the management protocol proxy server 60b, the transmitting origin currently held as transmission destination [in the header of IP layer which is a network layer], and transmitting origin stores transmission destination information in the management protocol proxy data which is equivalent to the data of the application layer. Connection-oriented TCP is used as the transport layer of the packet of management protocol proxy data. Transmission destination [of the management protocol proxy data itself] and transmitting origin serves as a management protocol proxy or a management protocol proxy server.

[0019]From the monitoring instrument 40 here to the node 50 or the node 90 which is a monitored device to the monitoring instrument 40 from the node 50 which is the opposite monitored device, or the node 90. Data flow in case communication is performed via the management protocol proxy 60a and the management protocol proxy server 60b is explained. When the data of a management protocol which the node 40 which is a monitoring instrument transmitted is sent to the management protocol proxy 60a, the management protocol proxy 60a, Management protocol proxy data is generated combining original transmission destination [of the data of a management protocol itself, and the data of a management protocol], and transmitting origin, and management protocol proxy data is transmitted to the management protocol proxy server 60b. From the received management protocol proxy data, the management protocol proxy server 60b takes out the data of a management protocol, and an original transmission destination, reconstructs the packet of a management protocol, and transmits to the node 50 which is a monitored device which is an original transmission destination. At this time, the response from the node 50 is transmitted to the management protocol proxy server 60b by what the transmitting origin of the packet of a management protocol is made into the management protocol proxy server 60b for. The management protocol proxy server 60b which received the response packet of the management protocol from the node 50 changes the response packet into management proxy protocol data, and returns it to the management protocol proxy 60a. The management protocol proxy 60a

reconstructs the response packet of a management protocol from management protocol proxy data, and returns it to the monitoring instrument 40.

[0020]In the environment which cannot carry out direct communication between nodes as mentioned above using a management protocol, communication by a management protocol can be performed now by passing a management protocol proxy and a management protocol proxy server.

[0021]The management protocol proxy and the management protocol proxy server have an address conversion function which changes the address of the PDU portion of a management protocol. By this the address of the node contained in the Protocol Data Unit ("PDU" is called hereafter.) of the management protocol of a node by changing into the virtual address for network management, It is manageable as if the node had a virtual address. The virtual address used only in the network management at this time is called an "administrative address" by this example for convenience.

[0022]In the composition shown by drawing 1, although the case where the management protocol proxy 60a was realized by a program was explained, the function of the management protocol proxy server 60b is realizable by a program similarly. In this case, a program is recorded on the magnetic disk which can be read, an optical disc, and a magneto-optical disc by computer, and the node which takes charge of the function of a management protocol proxy server reads and executes a program.

[0023]Next, NAT shown in drawing 1 is explained. NAT shown in drawing 1 is semi-*(ed) to RFC1631. Drawing 4 is a figure for explaining the function of NAT. In the network to which the global network 10 and the private network 30 are connected via NAT20 as shown in this figure, G0 is assigned as the global address 200, and the node 40 explains a monitored device about the case where L1 is assigned as the private address 210, and G1 is assigned as a global address. In this case, the conversion table 230 which that global address and a private address matched is formed in NAT20. This transmits a packet to the node 50 side from the node 40 side to the address G1. NAT20 changes a transmission destination address into L1 from G1 according to the conversion table 230, and transmits the packet towards the address G1 to the private network side. Namely, as a packet which arrived from the node 40 side to NAT20 like drawing 5, What was a packet containing the information of G1 a transmission destination as header information of IP layer portion equivalent to a network layer, When hooking up from NAT20 towards the node by the side of a private network, like drawing 6, as header information of IP layer portion, a transmission destination becomes a packet containing the information of L1, and is transmitted. When transmitting a packet towards the node 40 by the side of global network from the node 50 by the side of a private network conversely, As a packet which arrived from the node 50 to NAT20, what was a packet containing the information of L1 a transmitting agency as header information of IP layer portion, When hooking up from NAT20 towards the node 40 by the side of global network, a transmitting agency is transmitted as a packet containing the information of G1 as header information of IP layer portion.

[0024]What is necessary is just to set up by such work of NAT20 as what has the private address L1 as setting out of the network of node 50 self, When it can communicate using the private address L1 when the node 50 and other devices in a private network communicate, and communicating between the devices by the side of global network further, it can communicate using the global address G1 assigned by NAT20.

[0025]Here, NAT was explained as what has the function to perform address translation of IP layer (address translation of the PDU portion of a management protocol cannot be performed.). In the network using such NAT, as already explained, the address of the PDU portion of a management protocol is changed in a management protocol proxy server.

[0026]Hereafter, a more concrete network system is explained. Drawing 7 is one of the examples of application in a network management system, and is the composition in the case of managing using the formal global address assigned to

the supervising side device as an address for network management.

[0027]Monitored device a 50a has L1 as the private address 210. Since an address called this L1 is a private address, it is an address which can be used only in private network B 30b.

[0028]As the address translation 230 in NAT20b, the global address G1 and the private address L1 are matched, and the address G1 is statically assigned to monitored device a 50a as a global address. In carrying out direct communication to the monitored device a50a from the global network 10 or the private network A30a, it communicates using the global address G1.

[0029]By matching the administrative address G1 and the private address L1 as the address translation 220 in the management protocol proxy 60b here. About the managed protocol data in which G1 is sent to the surveillance side by L1 from a supervising side about the managed protocol data sent to a supervising side from the surveillance side, L1 is changed into G1, respectively.

[0030]Thereby, when the data of a management protocol is referred to from the monitoring instrument side using a management protocol, it is visible as if the monitored device a50a had the address G1.

[0031]For this reason, as the management information 240 in the monitoring instrument 40, the monitored device a is matched as it is a device with the address G1, and it can perform network management using the address G1.

[0032]Next, drawing 8 is a case where the global address assigned to a monitored device by NAT20b is assigned dynamically. There are few global addresses which can generally be used in the private network connected by NAT for external connection than the number of the devices in a private network. If assignment of the global address to a device is assigned as a method for utilizing few global addresses effectively only while the device has connected outside, and the device ends connection with the exterior, The method reused by other devices in the global address which the device was using is used. Thus, when assigning a global address dynamically, the global address generally assigned to one certain device changes with those times.

[0033]In such a case, as the address translation 230 in NAT20b, The global address Gx and the private address L1 are matched, Gx is an address which chooses and is chosen from the addresses of each time more fixed choice, and the address Gx will be dynamically assigned to the monitored device a50a at least as a global address at the time. It is determined by NAT20b what kind of address is assigned.

[0034]temporarily, supposing it uses Gx as it is as an administrative address, since [the] it sometimes comes out, and it can change, the continuity of management cannot be maintained and right network management cannot be performed, the address matched with the monitored device a50a as the management information 240 in the monitoring instrument 40 is a problem here.

[0035]Then, as the address translation 220 in the management protocol proxy 60b, a virtual address called V1 [completely different from Gx] is statically assigned like drawing 8. Since the monitored device a is matched with a thing with the address V1 as the management information 240 in a monitoring instrument by this, network management can be performed correctly.

[0036]The private network of drawing 9 of a supervising side is an example when the private address of the monitored device in those with two or more and these private networks is competing.

[0037]The monitored device b50b exists in the private network B30b, and has the private address L1. The monitored device c50c exists in the private network C30c, and has the private address L1. Although the mutual address is competing, since a private address is used only in the private network in a communication top, a network does not get confused.

[0038]however -- if the data of a management protocol is acquired from the monitored device b50b and the monitored device c50c using a direct management protocol -- which [the] -- although, in order to answer the information as a

device with the address L1, A monitoring instrument gets confused and the problem that network management is correctly impossible occurs.

[0039]Then, like drawing 9 about the monitored device b50b. In the address translation 220b in the management protocol proxy 60b, match the administrative address V1 and the private address L1, and about the monitored device c50c. In the address translation 220c in the management protocol proxy 60c, the administrative address V2 and the private address L1 are matched. That is, the administrative address V2 is statically assigned to the monitored device b50b at the administrative address V1 and the monitored device c50c, respectively.

[0040]As the management information 240 in a monitoring instrument, as a device with the address V1, the monitored device c is matched by this as a device with the address V2, respectively, and the monitored device b can perform network management correctly by it.

[0041]In a private network, the global address is not assigned, i.e., the exterior of drawing 10 is an example in the case of assigning and carrying out network management of the administrative address also to the device which is not connected.

[0042]The monitored device a50a has L1 as the private address 210a. As the address translation 230 in NAT20b, the global address G1 and the private address L1 are matched, and the address G1 is statically assigned to monitored device a 50a as a global address. In carrying out direct communication to the monitored device a50a from the global network 10 or the private network A30a, it communicates using the global address G1.

[0043]The monitored device b50b has L2 as the private address 210b. However, as the address translation 230 in NAT20b, The global address corresponding to the private address L2 is not defined, and, for this reason, direct communication can be carried out to the monitored device b50b from neither the global network 10 nor the private network A30a. However, the monitoring instrument 40 can exchange the information according to a management protocol in the monitored device 50b through a management protocol proxy even in this case.

[0044]At this time, the administrative address V2 and the private address L2 are matched for the administrative address V1 and the private address L1 in the address translation 220 in the management protocol proxy 60b, respectively. That is, the administrative address V1 is assigned to the monitored device a50a, and the administrative address V2 is statically assigned to the monitored device b50b, respectively. Thereby, as the management information 240 in a monitoring instrument, as a device in which the monitored device a50a has the address V1, the monitored device b50b is matched as a device with the address V2, respectively, and network management is performed.

[0045]Also as opposed to the device which the global address is not assigned, i.e., drawing 11 does not connect with the exterior in a private network, When assigning and carrying out network management of the administrative address, it is an example using an address virtual about the device to which uses a global address for an administrative address and the global address is not assigned about the device to which the global address is assigned.

[0046]The monitored device a50a has L1 as the private address 210a. As the address translation 230 in NAT20b, the global address G1 and the private address L1 are matched, and the address G1 is statically assigned to monitored device a 50a as a global address. In carrying out direct communication to the monitored device a50a from the global network 10 or the private network A30a, it communicates using the global address G1.

[0047]The monitored device b50b has L2 as the private address 210b. However, as the address translation 230 in NAT20b, The global address corresponding to the private address L2 is not defined, and, for this reason, direct communication can be carried out to the monitored device b50b from neither the global network 10 nor the private network A30a. However, the monitoring instrument 40 can exchange the information according to a management protocol in the monitored device 50b through a management protocol proxy even in this case.

[0048]At this time, the administrative address V2 and the private address L2 are matched for the administrative address G1 and the private address L1 in the address translation 220 in the management protocol proxy 60b, respectively. That is, the administrative address G1 is assigned to the monitored device a50a, and the administrative address V2 is statically assigned to the monitored device b50b, respectively. Thereby, as the management information 240 in a monitoring instrument, as a device in which the monitored device a50a has the address G1, the monitored device b50b is matched as a device with the address V2, respectively, and network management is performed.

[0049]Then, the composition of a management protocol proxy is explained using drawing 12 and drawing 13. Drawing 12 is the composition of the management protocol proxy of a supervising side.

[0050]The management protocol proxy 60b of a supervising side, The communications department 61 between proxies which processes establishment of the communication path 70 between proxies between the management protocol proxies 60a by the side of surveillance, and transmission and reception of management protocol proxy data, The proxy data assembly decomposition part 62 which processes the disassembly and assembly of management protocol proxy data, The address translation treating part 63 which carries out address translation of the address information in PDU of a management protocol, It becomes the ASN.1MIB definition statement 64 and the address translation definition 65 used as the input to an address translation treating part from the SNMP message transmission and reception section 66 which transmits and receives an SNMP message between monitored devices.

[0051]If the message of the management protocol which the monitoring instrument 40 published is changed into management protocol proxy data by the management protocol proxy 60a by the side of surveillance and is transmitted to the management protocol proxy of a supervising side, First, the communications department 61 between proxies receives the transmitted management protocol proxy data, and hands the proxy data assembly decomposition part 62. The proxy data assembly decomposition part 62 disassembles the received management protocol proxy data, and passes it address translation treating part 63. According to the ASN.1MIB definition statement 64 and the address translation definition 65, the address translation treating part 63, Address translation of the address information in the transmitting agency address information of the passed management protocol proxy data, transmission destination address information, and also PDU of a management protocol is carried out, and a conversion result is passed to the proxy data disassembly-and-assembly part 62. Out of proxy data, the proxy data assembly decomposition part 62 takes out PDU of transmission destination information, transmission source information, and a management protocol, and passes it to the SNMP message transmission and reception section 66. The SNMP message transmission and reception section 66 transmits PDU of a management protocol to the monitored device 50 specified as the transmission destination. That is, an SNMP message is transmitted. The monitored device 50 returns the response corresponding to the transmitted SNMP message to the SNMP message transmission and reception section 66. The SNMP message transmission and reception section 66 passes the SNMP message of a response which received, and the information of the transmitting origin and a transmission destination to the proxy data assembly decomposition part 62. Furthermore, as for a proxy data assembly decomposition part, transmission destination and transmitting origin passes PDU of the management protocol which is a response to an address translation treating part. According to the ASN.1MIB definition statement 64 and the address translation definition 65, the address translation treating part 63, Address translation of the address information in the transmitting agency address information of the passed management protocol proxy data, transmission destination address information, and also PDU of a management protocol is carried out, and a conversion result is passed to the proxy data disassembly-and-assembly part 62. Furthermore, as for the proxy data disassembly-and-assembly part 62, transmission destination and transmitting origin assembles PDU of a management

protocol as management protocol proxy data, and it passes it to the communications department 61 between proxies. The communications department 61 between proxies transmits management protocol proxy data to the management protocol proxy 60a by the side of surveillance, and the management protocol proxy 60a by the side of surveillance returns PDU of a management protocol to the monitoring instrument 40.

[0052]The place whose ASN.1MIB definition statement 64 is a standard describing method of the MIB object indicated to RFC1212 (Concise MIB Definitions) etc. here, It is the MIB definition statement described by ASN.1 (Abstract Syntax Notation One= abstract syntax notation.1). Generally, the MIB definition statement by ASN.1 is widely exhibited by those who defined the MIB module. In this example, in order to change the address included in Variable-bindings of the Protocol Data Unit of a management protocol using the information acquired by analyzing the MIB definition statement by ASN.1, special definition statement becomes unnecessary and composition becomes easier.

[0053]Drawing 13 is the composition of the management protocol proxy by the side of surveillance. The SNMP message transmission and reception section 66 in which the management protocol proxy 60a by the side of surveillance transmits and receives an SNMP message among the SNMP surveillance managers 41 on the monitoring instrument 40, It consists of the communications department 61 between proxies which processes establishment of the communication path 70 between proxies between the proxy data assembly decomposition part 62 which processes the disassembly and assembly of management protocol proxy data, and the management protocol proxy 60b of a supervising side, and transmission and reception of management protocol proxy data. If the SNMP message which the SNMP surveillance manager 41 on the monitoring instrument 40 published is passed to the management protocol proxy 60a by the side of surveillance, the SNMP message transmission and reception section 66 will receive an SNMP message, and will pass it to the proxy data assembly decomposition part 62. From the passed SNMP message, and the transmission destination and transmission source information, the proxy data assembly decomposition part 62 assembles management protocol proxy data, and passes it to the communications department 61 between proxies. The communications department 61 between proxies transmits the passed management protocol proxy data to the management protocol proxy 60b of a supervising side. Furthermore, the communications department 61 between proxies receives the management protocol proxy data of a response returned from the management protocol proxy 60b of a managing side, and hands the proxy data assembly decomposition part 62. As for the proxy data assembly decomposition part 62, a transmitting agency takes out a transmission destination and an SNMP message from management protocol proxy data, and it passes them to the SNMP message transmission and reception section 66. An SNMP message transmission and reception section returns an SNMP message to the SNMP surveillance manager 41 on the monitoring instrument 40 according to the passed information.

[0054]Drawing 14 is an example in case it is an example of the management protocol proxy data transmitted and received on the communication path 70 between proxies between the management protocol proxy 60a by the side of management, and the management protocol proxy 60b of a managing side and a management protocol is SNMP. In this case, as for management protocol proxy data, the transmitting origin of an SNMP message is a transmission destination of an SNMP message, and data which consists of SNMP PDU.

[0055]Drawing 2 is a figure of the packet of the usual SNMP message. The packet shows only the portion of the higher rank from IP layer which is a network layer. In transmitting-on IP layer level origin, in the usual SNMP packet, transmission destination information is [transmitting origin of the SNMP message itself] a transmission destination as it is.

[0056]Drawing 3 is a figure of the packet of management protocol proxy data in case a management protocol is SNMP. The packet shows only the portion of the higher rank from IP layer which is a network layer. In the packet of management protocol proxy data, The transmission destination of transmitting-on IP layer

level origin is one of the management protocol proxies which exist in the both ends of the communication path 70 between proxies, and, as for the transmitting origin of an SNMP message, the data of a transmission destination is contained in a packet as management protocol proxy data equivalent to the application layer. Therefore, the virtual address used for address translation is not used as the transmission destination or transmission source address of a actual communication packet. For this reason, even if it uses the virtual address which is not assigned from organizations, such as NIC, to the self-organization, it does not interfere with communication by IP layer, i.e., a network layer level, at all.

[0057]Thus, by the SNMP message transmitting origin on management protocol proxy data carrying out address translation of the transmission destination address, The virtual address which is not a formal global address can be used for an administrative address, even a device without a global address can include, and network management of the private network can be carried out.

[0058]The proxy data assembly decomposition part 62 is explained using drawing 15, drawing 16, drawing 17, and drawing 18. Drawing 15 is the composition of the proxy data assembly decomposition part 62.

[0059]The proxy data assembly decomposition part 62 consists of the partner proxy definition 69 which defined matching with the assembly decomposition treatment part 68 which performs assembly decomposition treatment, and the transmission destination address of an SNMP message and the partner proxy which should transmit the SNMP message.

[0060]Drawing 16 is an example of a definition of a partner proxy definition. The definition line 311 is a definition line showing an address transmitting the SNMP message whose 1st octet of a transmission destination address is 100 to the management protocol proxy of 200.10.20.30.

[0061]The 1st octet of a transmission destination address of the definition line 312 is a definition line showing an address transmitting the SNMP message 101 and whose 2nd octet are 10 to the management protocol proxy of 200.10.20.30.

[0062]The 1st octet of a transmission destination address of the definition line 313 is a definition line to which, as for the SNMP message 20 and whose 3rd octet 110 and the 2nd octet are 80, an address means transmitting to the management protocol proxy of 230.51.62.72.

[0063]The definition line 314 is a definition line showing an address transmitting the SNMP message whose transmission destination address is 120.60.11.8 to the management protocol proxy of 230.51.62.72. A transmission destination address is expressed using an administrative address at this time.

[0064]Drawing 17 is a flow chart of proxy data assembly processing. An SNMP message is received from an SNMP message transmission and reception section at Step 151. A transmission source address and a transmission destination address are taken out from the IP header part of an SNMP message at Step 152. SNMP PDU is taken out from an SNMP message at Step 153. The transmission source address and transmission destination address which were taken out at Step 154, and SNMP PDU are stored in management protocol proxy data. The partner proxy address matched with the transmission destination address which Step 155 was partner proxy defining and was taken out from the IP header part of the SNMP message is searched, and the partner proxy address is determined as the transmission destination of protocol proxy data. A proxy data assembly decomposition part assembles management protocol proxy data as mentioned above.

[0065]Drawing 18 is a flow chart of proxy data decomposition treatment. Management protocol proxy data and the address of the management protocol proxy which is the partner who transmitted the management protocol proxy data are received from the communications department between proxies at Step 161. A transmission source address, a transmission destination address, and SNMP PDU are taken out from management protocol proxy data at Step 162. The transmission source address and transmission destination address which were taken out at Step

163 are stored in the IP header part of an SNMP message. SNMP PDU taken out at Step 164 is stored in an SNMP message. A proxy data assembly decomposition part disassembles management protocol proxy data as mentioned above.

[0066]Drawing 19 is a figure showing the composition of the address translation treating part 63. The address translation treating part 63 consists of the SNMP message transmitting former transmission destination address converter 85 which changes the address of a transmission destination, and the PDU address conversion section 80 which changes the address information contained in SNMPPDU the transmitting origin of an SNMP message. The PDU analysis converter 81 in which the PDU address conversion section 80 furthermore processes the analysis and address translation of PDU, The object identifier address conversion section 82 which processes conversion of the address included as an object identifier among the address information contained in PDU, It consists of the trap transmission source address converter 84 which processes conversion of the address included as a trap transmission source address among the MIB value address conversion section 83 which processes conversion of the address included as an MIB value among the address information contained in PDU, and the address information contained in PDU.

[0067]From the proxy data assembly decomposition part 62, if management protocol proxy data is passed to the address translation treating part 63, In the SNMP message transmitting origin in management protocol proxy data, the SNMP message transmitting former transmission destination address converter 85 performs address translation about a transmission destination according to the address translation definition 65 first. Next, the SNMP message transmitting former transmission destination address converter 85 passes management protocol proxy data to the PDU analysis converter 81. The PDU analysis converter 81 analyzes about PDU in the passed management protocol proxy data, and extracts the portion which needs address translation from the inside. First, a trap transmission source address portion is extracted from PDU, the trap transmission source address converter 84 is passed, and the trap transmission source address converter 84 carries out address translation of the trap transmission source address according to the address translation definition 65, and returns it to the PDU analysis converter 81. The PDU analysis converter 81 is an address after the conversion received from the trap transmission source address converter 84, and replaces the trap transmission source address portion of PDU. The classification of data extracts the MIB value which is a thing showing an IP address from PDU, the MIB value address conversion section 83 is passed, and the MIB value address conversion section 83 carries out address translation of the MIB value according to the address translation definition 65, and returns it to the PDU analysis converter 81. The PDU analysis converter 81 is an address after the conversion received from the MIB value address conversion section 83, and replaces the MIB value portion of PDU. Extract the object identifier of MIB from PDU, pass the object identifier address change part 82, and the object identifier address conversion section 82, Address translation of the IP address included in an object identifier according to ASN.1MIB definition statement and the address translation definition 65 is carried out, and it returns to the PDU analysis converter 81. The PDU analysis converter 81 is an address after the conversion received from the object identifier address conversion section 82, and replaces the object identifier portion of MIB of PDU. Finally a PDU analysis converter returns the management protocol proxy data having contained PDU after performing address translation to the proxy data assembly decomposition part 62. The address translation treating part can perform address translation about the data of a management protocol as mentioned above.

[0068]Drawing 20 is the composition of the object identifier address conversion section 82. The ASN.1MIB definition statement decoding section 88 in which the object identifier address conversion section 82 decodes the ASN.1MIB definition statement 65, The object identifier extraction part 89 for conversion which extracts the object which needs to change an object identifier based on the definition content of decoded MIB, The object identifier passed from the PDU

analysis converter 81 is compared with the object identifier which the object identifier extraction part 89 for conversion extracted, It consists of the address translation execution part 87 which carries out address translation of the object identifier based on the object identifier comparing element 86 which judges whether the passed object identifier needs to be changed, and the defining information and the address translation definition 65 which the object identifier extraction part for conversion extracted.

[0069]First, the information on the MIB definition obtained as a result of the ASN.1MIB definition statement decoding section's 88 reading, decoding and decoding the ASN.1MIB definition statement 65 is passed to the object identifier extraction part 89 for conversion. The object identifier extraction part 89 for conversion extracts the MIB object which may include an IP address in an object identifier out of the passed MIB definition, The INDEX information which is the defining information of the MIB object which corresponds the list of the object identifiers of an applicable MIB object to the object identifier comparing element 86 is passed to the address translation execution part 87, respectively. Here with the MIB object which may include an IP address in an object identifier. It is an MIB [of as / whose one or more of the MIB objects in an MIB table used as INDEX of a table it is an MIB object showing an MIB table, and are IP addresses] object. Such an object, When acquiring the instance which is a value of an MIB object at a GET request etc., add INDEX which is an instance identifier after the object identifier of an MIB object, and specify as one object identifier, but. Since an IP address is used for INDEX at this time, an IP address may be included in an object identifier. As INDEX information passed to the address translation execution part 87, When two or more MIB objects are matched as INDEX of an MIB table, in order to change only the portion of the IP address in it, the information which arranged in order SYNTAX which is the classification of the MIB object used as INDEX is passed. For example, in the case of an MIB table which takes one integral MIB object and IP address, an instance identifier turns into an identifier with a total of five subidentifiers of four parts of one and the IP address of an integral part as INDEX. In address translation, since it is necessary to interpret the 2nd to the 5th subidentifier of these as an IP address, and to change it, INDEX needs to pass the information that it is a group of one integer and one IP address to the address translation execution part 87.

[0070]Now, if the object identifier in PDU is passed to the object identifier address conversion section 82 from the PDU analysis converter 81, the object identifier comparing element 86 will receive an object identifier first here. The object identifier to which the object identifier comparing element 86 was passed from the PDU analysis converter 81, The object identifier list for [which the object identifier extraction part 89 for conversion extracted] conversion is compared, If the object identifier passed from the PDU analysis converter 81 is contained in the object identifier list for conversion, an object identifier will be passed to the address translation execution part 87 from the PDU analysis converter 81. If the object identifier passed from the PDU analysis converter 81 is not contained in the object identifier list for conversion, the object identifier passed from the PDU analysis converter 81 will be returned to the PDU analysis converter 81 as it is, without changing anything.

[0071]Next, the address translation execution part 87 about the passed object identifier. The position of the IP address which appears in an object identifier based on the INDEX information first passed from the object extraction part 89 for conversion, That is, transformation positions are pinpointed, then, address translation is performed based on the address translation definition 65, and the object identifier after conversion is returned to the PDU analysis converter 81.

[0072]Address translation of the IP address by which an object identifier address conversion section is contained as mentioned above in the object identifier of MIB can be carried out.

[0073]Processing of a PDU analysis converter is explained using the flow chart of

drawing 21. The data which expresses the PDU classification from PDU with Step 111 is extracted. The direction of address translation is determined from PDU classification at Step 112. The direction of address translation means whether to change into an administrative address from a real address whether the address in PDU is changed into a real address from an administrative address. PDU transmitted to a supervising side changes an administrative address into a real address from the surveillance side. PDU transmitted to the surveillance side changes a real address into an administrative address from a supervising side. Since it was decided for every PDU classification, whether it is transmitted from a supervising side to the surveillance side whether it is transmitted to a supervising side from the surveillance side can determine the direction of address translation from PDU classification according to the table of drawing 22. It is judged at Step 113 whether the classification of PDU is an SNMP trap. In the case of an SNMP trap, it progresses to Step 114. When it is not an SNMP trap, it progresses to Step 117. At Step 114, a trap transmission source address is extracted from PDU. At Step 115, the information on the direction of address translation it was determined at a trap transmission source address and Step 112 that extracted at Step 114 is passed to a trap transmission source address converter, and the trap transmission source address after conversion is received. At Step 116, the trap transmission source address of PDU is transposed to the trap transmission source address after the conversion received at Step 115. At Step 117, it is judged whether variableBindingList exists in PDU. When variableBindingList exists, it progresses to Step 118. When variableBindingList does not exist, processing of a PDU analysis converter is ended. At Step 118, one variableBind which has not been processed yet is extracted from variableBindingList. At Step 119, an object identifier and a value are extracted from variableBind extracted at Step 118. At Step 120, the MIB value extracted at Step 119 and the information on the conversion direction determined at Step 112 are passed to an MIB value address conversion section, and the MIB value after conversion is received. At Step 121, the object identifier extracted at Step 119 and the information on the conversion direction determined at Step 112 are passed to an object identifier address conversion section, and the object identifier after conversion is received. At Step 122, the MIB value of variableBind is transposed to the MIB value after the conversion received at Step 120 at the object identifier after the conversion which received the object identifier of variableBind of PDU at Step 121, respectively. It is judged whether at Step 123, unsettled variableBinding still remains. If it remains, it will progress to Step 118. If it does not remain, processing of a PDU analysis converter will be ended. The address information in PDU is convertible as mentioned above. Processing of the object identifier extraction part for conversion is explained using the flow chart of drawing 23.

[0074] One object identifier defined as MIB definition statement at Step 131 is taken out. The object identifier taken out in Step 131 at Step 132 judges whether it is an identifier showing an MIB table. In the case of the identifier showing an MIB table, it progresses to Step 133. When it is not an identifier showing a Mib table, it progresses to Step 136. At Step 133, SYNTAX of the MIB object in a table specified as INDEX of an object identifier is extracted. It is also judged whether the number of what is SYNTAX(s) to which SYNTAX of the MIB object in a table extracted in Step 133 expresses an IP address with Step 134 is one. In a certain case, it progresses to Step 135. When there is nothing, it progresses to Step 136. It is judged that the object identifier taken out in Step 131 at Step 135 is an object identifier for conversion.

[0075] It is judged that the object identifier taken out in Step 131 at Step 136 is not an object identifier for conversion. At Step 137, it is judged whether an unsettled object identifier is still in MIB definition statement. In a certain case, it still progresses to Step 131. When there is nothing, it progresses to Step 138. At Step 138, all the object identifiers judged to be the candidates for conversion are notified to an object identifier comparing element. At Step 139, all the INDEX information on an object identifier judged to be the candidates for

conversion is notified to an address translation execution part. Processing of the object identifier extraction part for conversion is realizable as mentioned above.

[0076]Drawing 24 is an example of a definition of the address translation definition 65. The definition line 301 is an example of a definition in the case of changing only the 1st octet of an IP address. In this case, that from which all the real addresses whose 1st octet is 10 changed the 1st octet into 100 serves as an administrative address. For example, when the address 100.1.2.3 is in the data of a management protocol transmitted from the monitoring instrument 40, by address translation, the address is changed into 10.1.2.3 and relayed to the monitored device 50. On the contrary, when the address 10.1.2.3 is during the response from the monitored device 50, by address translation, the address is changed into 100.1.2.3 and relayed to the monitoring instrument 40. The definition line 302 is an example of a definition in the case of changing the 1st octet and the 2nd octet of an IP address. In this case, the 1st octet is 172 and what all the real addresses whose 2nd octet is 16 changed the 1st octet into 101, and changed the 2nd octet into 10 serves as an administrative address. For example, when the address 101.10.1.2 is in the data of a management protocol transmitted from the monitoring instrument 40, by address translation, the address is changed into 172.16.1.2 and relayed to the monitored device 50. On the contrary, when the address 172.16.1.2 is during the response from the monitored device 50, by address translation, the address is changed into 101.10.1.2 and relayed to the monitoring instrument 40. The definition line 303 is an example of a definition in the case of changing the 1st octet, the 2nd octet, and the 3rd octet of an IP address. In this case, the 1st octet is 172, the 2nd octet is 17 and what all the real addresses whose 3rd octet is 50 changed the 1st octet into 110, changed the 2nd octet into 20, and changed the 3rd octet into 80 serves as an administrative address. For example, when the address 110.20.80.1 is in the data of a management protocol transmitted from the monitoring instrument 40, by address translation, the address is changed into 172.17.50.1 and relayed to the monitored device 50. On the contrary, when the address 172.17.50.1 is during the response from the monitored device 50, by address translation, the address is changed into 110.20.80.1 and relayed to the monitoring instrument 40. The definition line 304 is an example of a definition in the case of changing all the octets of the 1st octet to the 4th octet of an IP address. In this case, the real address whose address is 192.168.20.5 is changed into the administrative address 120.60.11.8. For example, when the address 120.60.11.8 is in the data of a management protocol transmitted from the monitoring instrument 40, by address translation, the address is changed into 192.168.20.5 and relayed to the monitored device 50. On the contrary, when the address 192.168.20.5 is during the response from the monitored device 50, by address translation, the address is changed into 120.60.11.8 and relayed to the monitoring instrument 40.

[0077]Drawing 25 is an example of composition of another virtual network management system. In this case, although the management protocol proxy 60a by the side of the monitoring instrument 40 and a monitoring instrument exists on the global network 10, it can perform virtual network management using an administrative address as well as the case of the composition of drawing 1 in any way.

[0078]Drawing 26 and drawing 27 are the composition of the management protocol proxy in another example, and are an example in the case of carrying out address translation by the management protocol proxy by the side of surveillance.

[0079]Address translation can be performed by the same method as the case where address translation is carried out by the management protocol proxy of the supervising side shown in drawing 12 and drawing 13 also in this case. However, when carrying out address translation in the management protocol proxy by the side of surveillance, The address translation definition defined as the management protocol proxy by the side of surveillance, A definition is

independently given for every private network of a supervising side, for example, the address translation definition 65b is defined for private network B of a supervising side, and the address translation definition 65c is defined for private network C of a supervising side, respectively. Even when the private address of a monitoring instrument is competing in two or more supervising side private networks like the composition of drawing 9 by this, it can be made to carry out address translation correctly.

[0080] Drawing 28 and drawing 29 are the composition of the virtual network managerial system in example another again, and the composition of the management protocol proxy of a managing side, and are the composition that it operates on the same device as NAT which the management protocol proxy of the managing side semi- *(ed) to RFC1631.

[0081] This example the management protocol proxy 60a by the side of the monitoring instrument 40 and surveillance, It is the composition that it operates on the same device as NAT20 which existed on the global network 10, and performed address translation by the management protocol proxy of the supervising side, and the management protocol proxy of the managing side semi- *(ed) to RFC1631.

[0082] Drawing 29 is the composition of the management protocol proxy 60b of the supervising side which operates on the same device as NAT20 which does not have an address conversion function of the management protocol which semi- *(ed) in RFC1631. When the communications department 61 between proxies communicates with the management protocol proxy 60a by the side of surveillance, Communicating via the global-network side communications protocol processing part 21 of NAT20, and when the SNMP message transmission and reception section 66 transmits and receives the monitored device 50 and data, It is the difference from the composition of drawing 12 to communicate via the private network side communications protocol processing part 23 of NAT20. About the packet which is going to pass through the device of NAT20 from the global-network side to the private network side, as a motion which semi- *(ed) to RFC1631 of NAT20. Catch the packet through which the global-network side communications protocol processing part 21 tends to pass first, and the RFC1631 semi- ** address translation treating part 22 is passed, After the RFC1631 semi- ** address translation treating part 22 carries out address translation, a packet is passed to the private network side communications protocol processing part 23, and it is sent out by the private network side communications protocol processing part 23 to the private network side.

[0083] About the packet which is going to pass from the private network side to the global-network side, on the contrary. Catch the packet through which the private network side communications protocol processing part 23 tends to pass first, and the RFC1631 semi- ** address translation treating part 22 is passed, After the RFC1631 semi- ** address translation treating part 22 carries out address translation, a packet is passed to the global-network side communications protocol processing part 21, and it is sent out by the global-network side communications protocol processing part 21 to the global-network side.

[0084] However, the communication by the communications department 61 between proxies is communication which carries out the address by the side of the global network of the device with which NAT and the management protocol proxy of a supervising side operate transmission destination or transmitting origin, and is not the communication which is going to pass through NAT20. For this reason, data is passed to the communications department 61 between proxies as it is from the global-network side communication processing part 21, without the RFC1631 semi- ** address translation treating part 22 passing.

[0085] It is the communication which carries out the address by the side of the private network of the device with which NAT and the management protocol proxy of a supervising side operate transmission destination or transmitting origin also with communication by the SNMP message transmission and reception section 66, and is not the communication which is going to pass through NAT20. For this reason,

data is passed to the SNMP message transmission and reception section 66 as it is from the private network side communication processing part 23, without the RFC1631 semi- ** address translation treating part 22 passing.

[0086]It is possible to realize operation, now virtual network management on the same device as NAT20 from the above thing using the management protocol proxy of the same composition as the management protocol proxy of the supervising side shown in drawing 12.

[0087]Processing of the management protocol proxy is realizable by a program as the flow chart showed it, as already stated.

[0088]as mentioned above, with the function in which NAT performs address translation of IP layer, although NAT explained as what performs address translation of IP layer (NAT changes the address of the PDU portion of a management protocol -- a functional owner has not been carried out.). When it has the function to change the address of the PDU portion of a management protocol, address translation of the PDU portion of a management protocol can be performed using NAT and a management protocol proxy server selectively.

[0089]

[Effect of the Invention]As explained above, data communications can be performed between the proxies of a management protocol, and the data communications by a management protocol can be performed between nodes without a global address.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the basic constitution of a network system.

[Drawing 2]It is a figure showing the composition of the packet of an SNMP message.

[Drawing 3]It is a figure showing the composition of the packet of management protocol proxy data.

[Drawing 4]It is a figure for explaining the function of NAT.

[Drawing 5]It is a figure showing the composition of the packet of an SNMP message.

[Drawing 6]It is a figure showing the composition of the packet of an SNMP message.

[Drawing 7]It is a figure showing the example of 1 application in a virtual network managerial system.

[Drawing 8]It is a figure showing the example of 1 application in a virtual network managerial system.

[Drawing 9]It is a figure showing the example of 1 application in a virtual network managerial system.

[Drawing 10]It is a figure showing the example of 1 application in a virtual network managerial system.

[Drawing 11]It is a figure showing the example of 1 application in a virtual network managerial system.

[Drawing 12]It is a figure showing the composition of the management protocol proxy of a supervising side.

[Drawing 13]It is a figure showing the composition of the management protocol proxy by the side of surveillance.

[Drawing 14]It is a figure showing an example of management protocol proxy data.

[Drawing 15]It is a figure showing the composition of a proxy data disassembly-and-assembly part.

[Drawing 16]It is a figure showing the example of a definition of a partner proxy

definition.

[Drawing 17] It is a figure showing the flow chart of proxy data assembly processing.

[Drawing 18] It is a figure showing the flow chart of proxy data decomposition treatment.

[Drawing 19] It is a figure showing the composition of an address translation treating part.

[Drawing 20] It is a figure showing the composition of an object identifier address conversion section.

[Drawing 21] It is a figure showing the flow chart of processing of a PDU analysis converter.

[Drawing 22] It is a figure showing the relation between the transmit direction of PDU classification and PDU, and the conversion direction of address translation.

[Drawing 23] It is a figure showing the flow chart of processing of the object identifier extraction part for conversion.

[Drawing 24] It is a figure showing the example of a definition of an address translation definition.

[Drawing 25] It is a figure showing the example of composition of a virtual network managerial system.

[Drawing 26] It is a figure showing the composition of a management protocol proxy.

[Drawing 27] It is a figure showing the composition of a management protocol proxy.

[Drawing 28] It is a figure showing the composition of a virtual network managerial system.

[Drawing 29] It is a figure showing the composition of the management protocol proxy of a managing side.

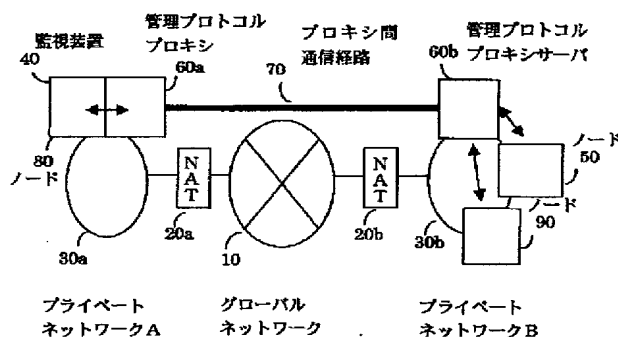
[Description of Notations]

10 [-- A monitoring instrument, 50 / -- A monitored device, 60 / -- A management protocol proxy, 70 / -- Communication path between proxies] -- Global network, 20 -- NAT, 30 -- A private network, 40

DRAWINGS

[Drawing 1]

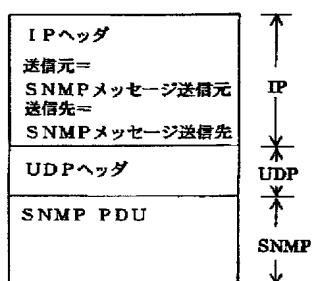
図1



[Drawing 2]

図2

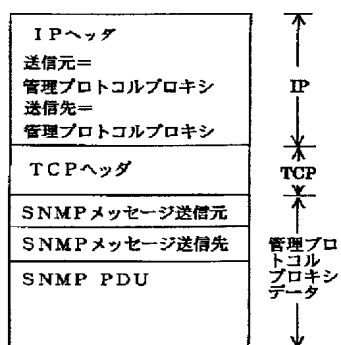
SNMP メッセージのパケット



[Drawing 3]

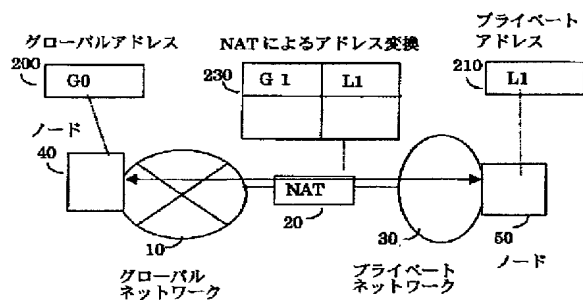
図3

管理プロトコルプロキシデータのバケット



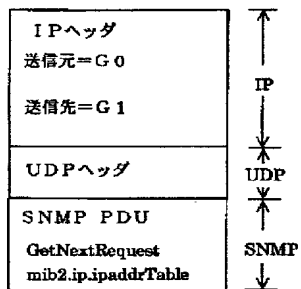
[Drawing 4]

図4



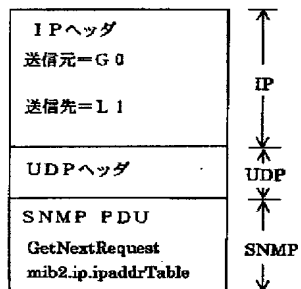
[Drawing 5]

図 5



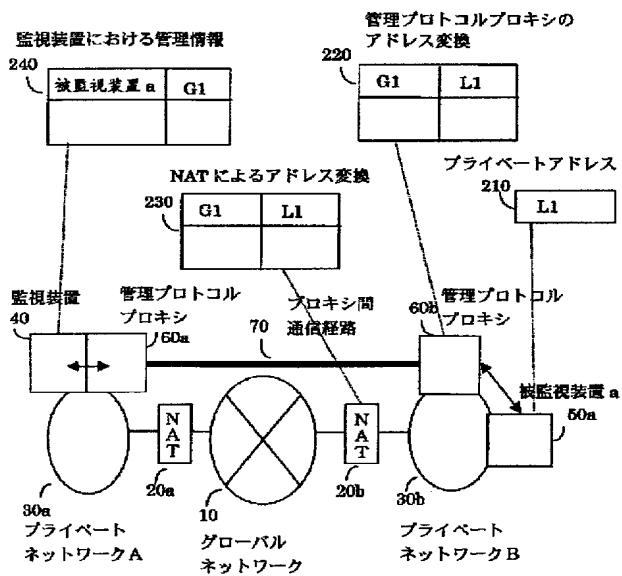
[Drawing 6]

図 6



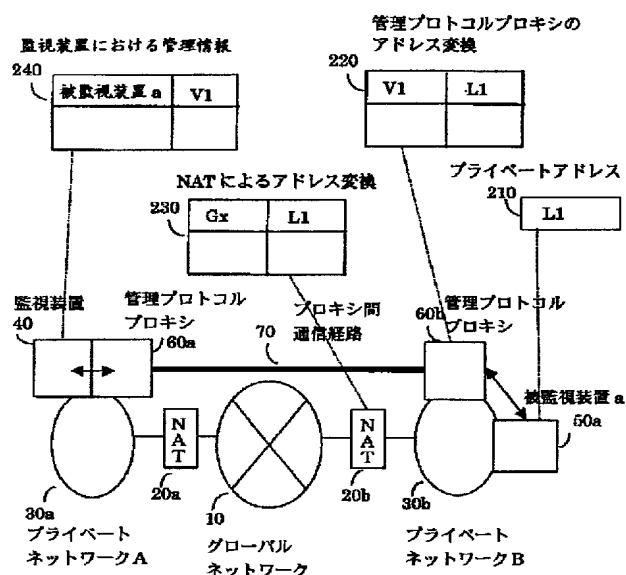
[Drawing 7]

図 7



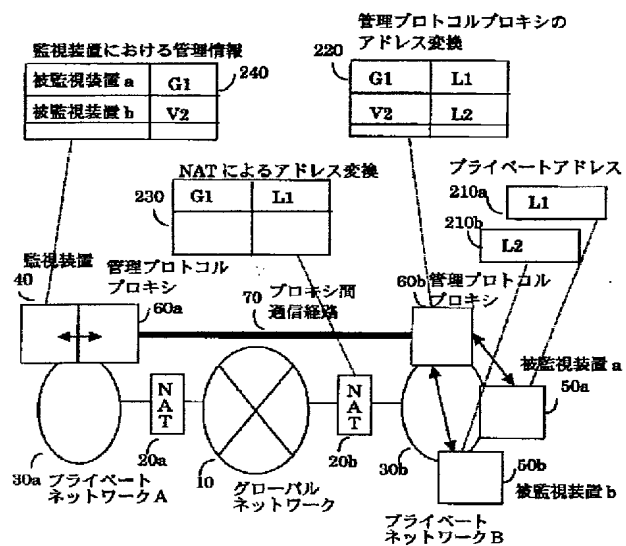
[Drawing 8]

図 8



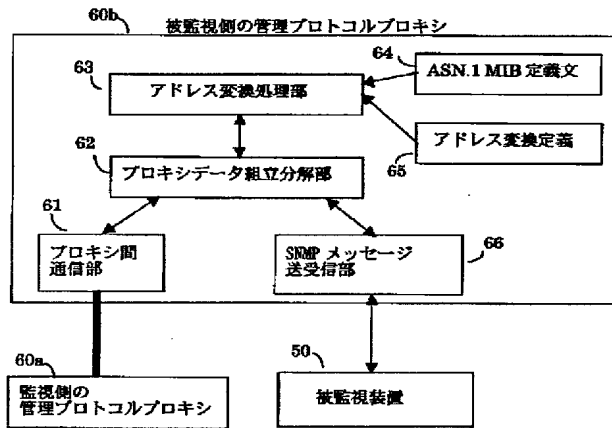
[Drawing 11]

図 11



[Drawing 12]

図 12

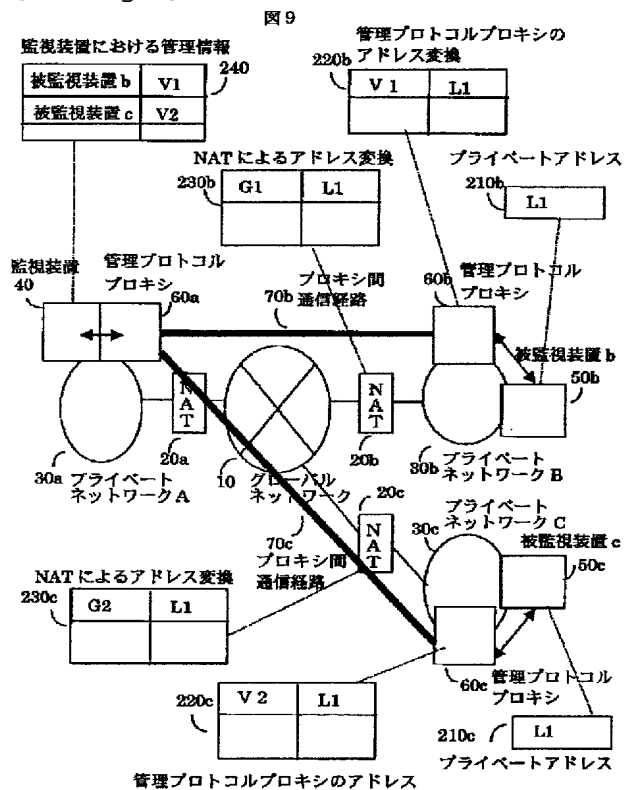


[Drawing 14]

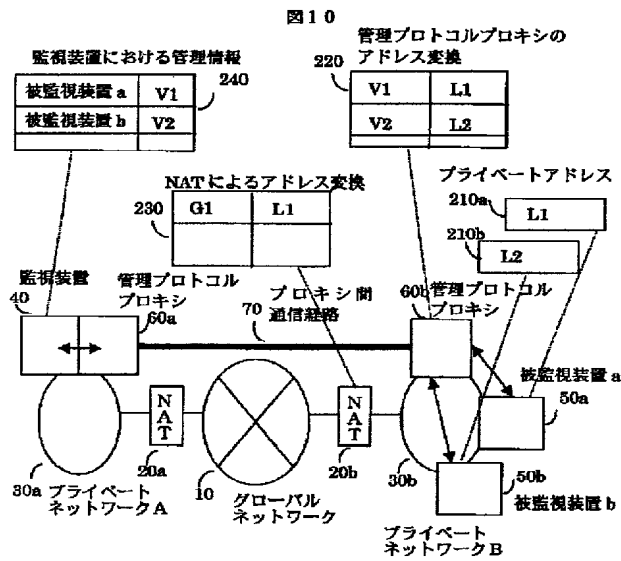
図 14

SNMPメッセージ送信元
SNMPメッセージ送信先
SNMP PDU

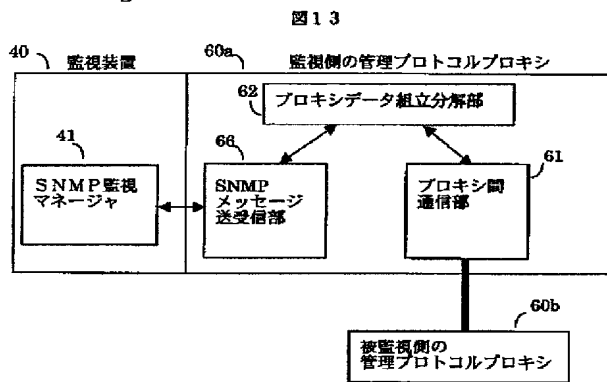
[Drawing 9]



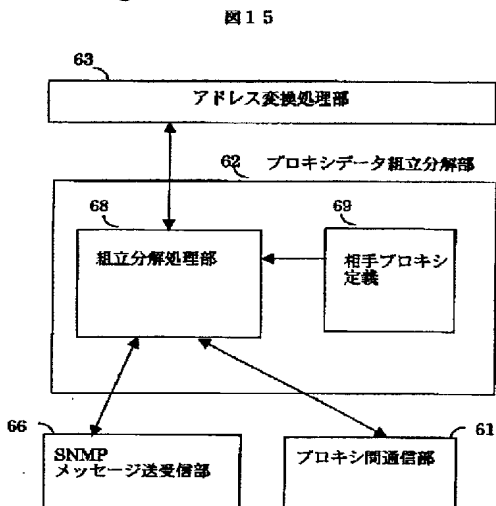
[Drawing 10]



[Drawing 13]



[Drawing 15]



[Drawing 16]

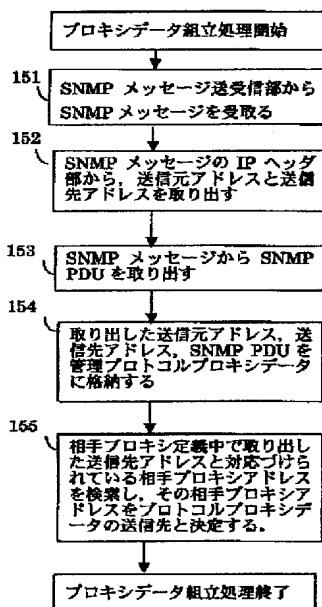
図 16

69 相手プロキシ定義

送信先アドレス	相手プロキシアドレス	
100. *. *. *	200. 10. 20. 30	311
101. 10. *. *	200. 10. 20. 30	312
110. 20. 80. *	210. 25. 15. 5	313
120. 60. 11. 8	230. 51. 62. 72	314

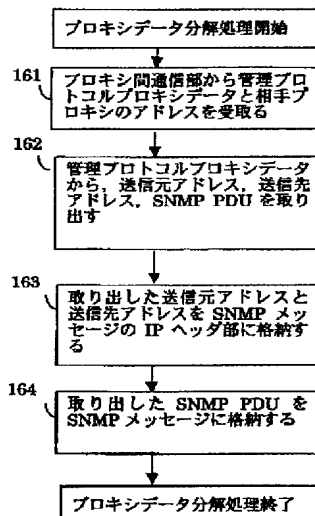
[Drawing 17]

図 17

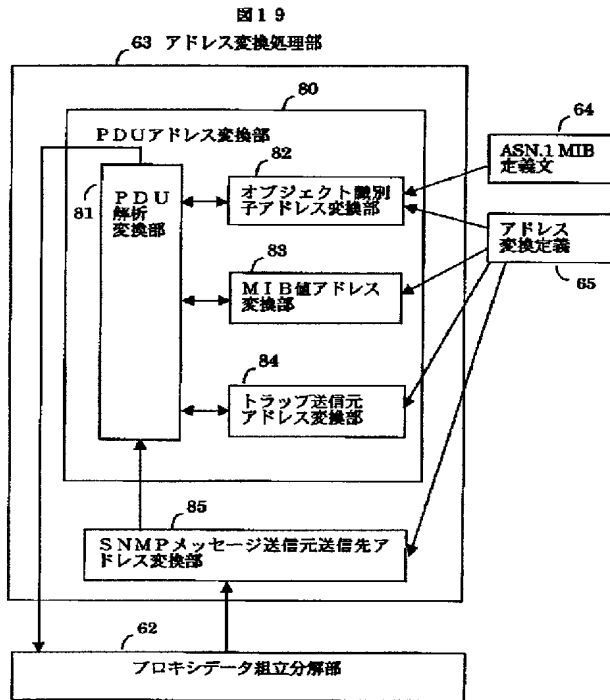


[Drawing 18]

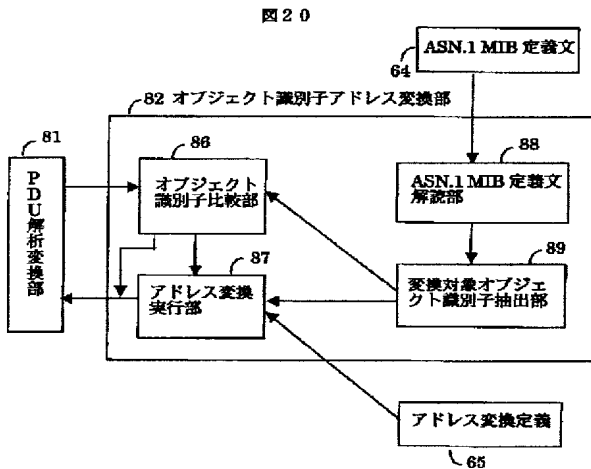
図 18



[Drawing 19]



[Drawing 20]



[Drawing 22]

図 22

送信方向	変換方向	PDU種別
監視装置側から被監視装置側へ送信	実アドレスから管理用アドレスへ変換	Get-Request, Getnext-Request, Set-Request
被監視装置側から監視装置側へ送信	実アドレスから管理用アドレスへ変換	Get-Response, Trap

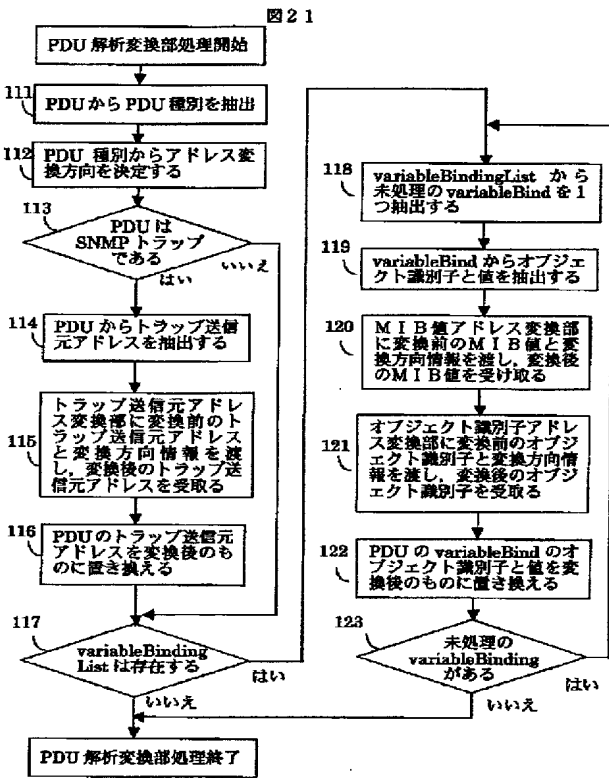
[Drawing 24]

図 2 4

65 アドレス変換定義

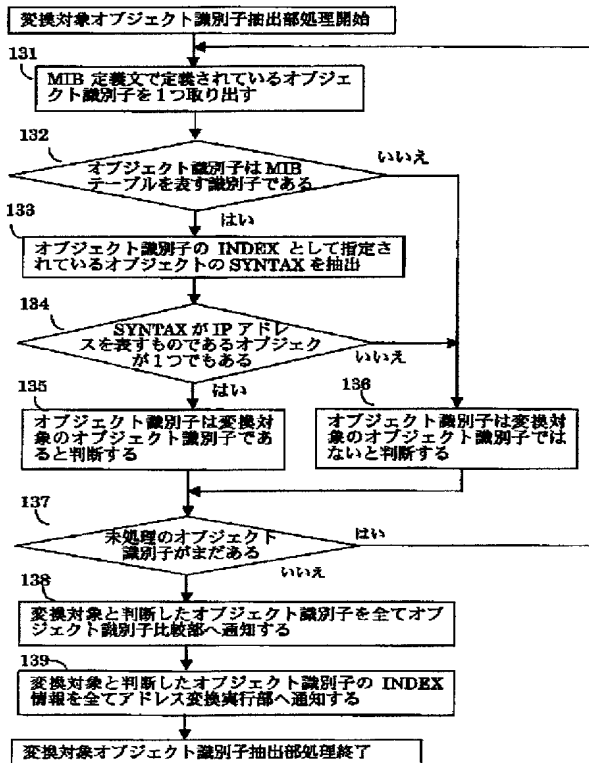
管理用アドレス	実アドレス	
100. *. *. *	10. *. *. *	301
101. 10. *. *	172. 16. *. *	302
110. 20. 80. *	172. 17. 50. *	303
120. 60. 11. 8	192. 168. 20. 5	304

[Drawing 21]



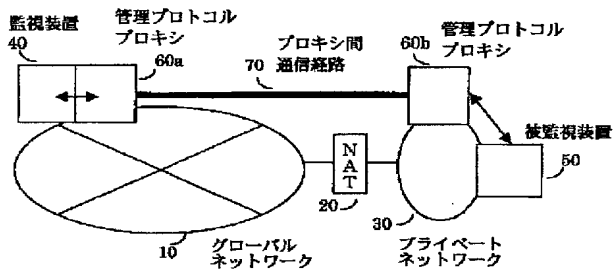
[Drawing 23]

圖 2 3



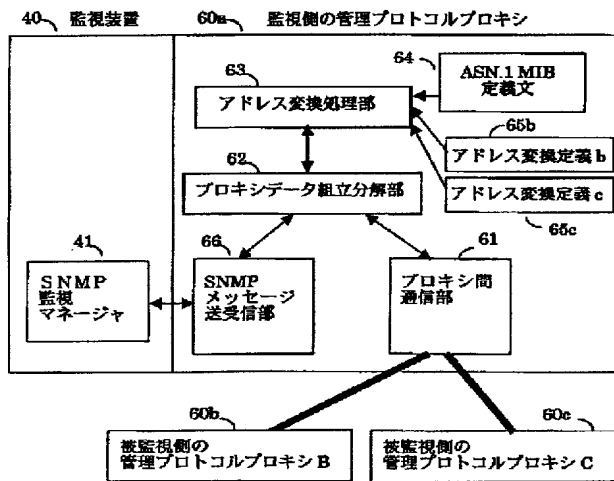
[Drawing 25]

图 25



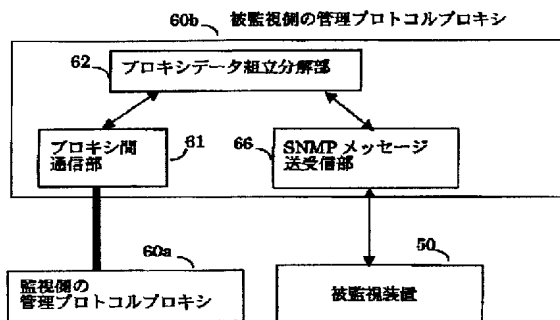
[Drawing 26]

図 2 6



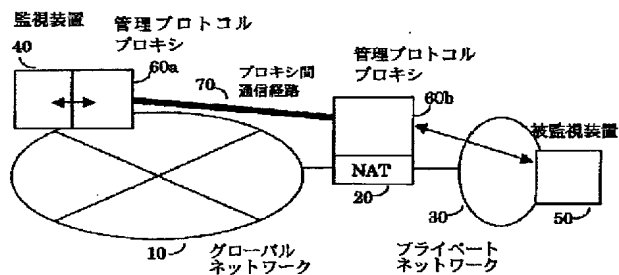
[Drawing 27]

図 2 7



[Drawing 28]

図 2 8



[Drawing 29]

